



CVE-2016-0225

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

Summary	
CVE	CVE-2016-0225
State	PUBLISHED
Assigner	ibm
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-02-29 11:59:07 UTC
Updated	2026-05-06 22:30:45 UTC
Description	IBM WebSphere Commerce 6.x through 6.0.0.11 and 7.x through 7.0.0.9 allows remote authenticated Commerce Accelerator users to bypass authentication and access the Commerce Accelerator REST API. This vulnerability is caused by a missing check for the user's authentication status in the Commerce Accelerator REST API. An attacker can exploit this vulnerability by sending a request to the Commerce Accelerator REST API with a valid user ID and password. The attacker can then bypass authentication and access the Commerce Accelerator REST API. This vulnerability can be exploited by an attacker who has access to the Commerce Accelerator REST API. The attacker can use this vulnerability to access sensitive information and perform unauthorized actions. The attacker can also use this vulnerability to escalate their privileges and gain access to the Commerce Accelerator REST API. This vulnerability is a result of a missing check for the user's authentication status in the Commerce Accelerator REST API. An attacker can exploit this vulnerability by sending a request to the Commerce Accelerator REST API with a valid user ID and password. The attacker can then bypass authentication and access the Commerce Accelerator REST API. This vulnerability can be exploited by an attacker who has access to the Commerce Accelerator REST API. The attacker can use this vulnerability to access sensitive information and perform unauthorized actions. The attacker can also use this vulnerability to escalate their privileges and gain access to the Commerce Accelerator REST API. This vulnerability is a result of a missing check for the user's authentication status in the Commerce Accelerator REST API.

Risk And Classification

Primary CVSS: v3.0 4.9 MEDIUM from nvd@nist.gov

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

Problem Types: CWE-200 | CWE-284 | n/a

Version	Source	Type	Score	Severity	Vector
3.0	nvd@nist.gov	Primary	4.9	MEDIUM	CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N
2.0	nvd@nist.gov	Primary	4		AV:N/AC:L/Au:S/C:P/I:N/A:N

CVSS v3.0 Breakdown	
Attack Vector	Network
Attack Complexity	Low
Privileges Required	High
User Interaction	None
Scope	Unchanged
Confidentiality	High
Integrity	None
Availability	

None

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

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

Single

Confidentiality

Partial

Integrity

None

Availability

None

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

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	7.0.0.9	All	All	All

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

References						
Reference						
IBM Security Bulletin: IBM WebSphere Commerce is vulnerable to an information disclosure vulnerability in the WebSphere Commerce Accelerator						
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.						