

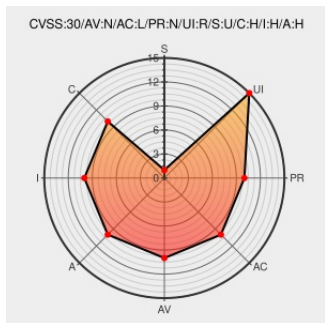


# CVE-2015-5007

Published on: 01/14/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:15 PM UTC

## CVE-2015-5007

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Websphere Commerce](#) from [Ibm](#) contain the following vulnerability:

Cross-site request forgery (CSRF) vulnerability in IBM WebSphere Commerce 6.0 through 6.0.0.11, 7.0 through 7.0.0.9, and 7.0 Feature Pack 8 allows remote authenticated users to hijack the authentication of arbitrary users for requests that insert XSS sequences.

CVE-2015-5007 has been assigned by [psirt@us.ibm.com](#) to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **8.8 - HIGH**

| Attack Vector    | Attack Complexity      | Privileges Required | User Interaction    |
|------------------|------------------------|---------------------|---------------------|
| <b>NETWORK</b>   | <b>LOW</b>             | <b>NONE</b>         | <b>REQUIRED</b>     |
| Scope            | Confidentiality Impact | Integrity Impact    | Availability Impact |
| <b>UNCHANGED</b> | <b>HIGH</b>            | <b>HIGH</b>         | <b>HIGH</b>         |

CVSS2 Score: **6.8 - MEDIUM**

| Access Vector          | Access Complexity | Authentication      |
|------------------------|-------------------|---------------------|
| <b>NETWORK</b>         | <b>MEDIUM</b>     | <b>NONE</b>         |
| Confidentiality Impact | Integrity Impact  | Availability Impact |
| <b>PARTIAL</b>         | <b>PARTIAL</b>    | <b>PARTIAL</b>      |

## CVE References

| Description                                                  | Tags                                                                                                    | Link                             |
|--------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|----------------------------------|
| IBM notice: The page you requested cannot be displayed       | <a href="#">www-01.ibm.com</a><br><a href="#">text/html</a><br><b>Inactive Link</b> <b>Not Archived</b> | <a href="#">AIXAPAR JR54268</a>  |
| IBM WebSphere Commerce Access Control Flaw Lets Remote Users | <a href="#">www.securitytracker.com</a>                                                                 | <a href="#">SECTrack 1034639</a> |

|                                                              |                                                                                              |                                                                            |
|--------------------------------------------------------------|----------------------------------------------------------------------------------------------|----------------------------------------------------------------------------|
| Conduct Cross-Site Request Forgery Attacks - SecurityTracker | text/html                                                                                    |                                                                            |
| IBM notice: The page you requested cannot be displayed       | Vendor Advisory<br><a href="#">www-01.ibm.com</a><br>text/html<br>Inactive Link Not Archived | CONFIRM <a href="#">www-01.ibm.com/support/docview.wss?uid=swg21972611</a> |
| IBM notice: The page you requested cannot be displayed       | <a href="#">www-01.ibm.com</a><br>text/html<br>Inactive Link Not Archived                    | AIXAPAR JR54267                                                            |

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to [comment@cve.report](mailto:comment@cve.report).

There are currently no QIDs associated with this CVE

| Known Affected Configurations (CPE V2.3) |             |                                    |          |                |         |          |
|------------------------------------------|-------------|------------------------------------|----------|----------------|---------|----------|
| Type                                     | Vendor      | Product                            | Version  | Update         | Edition | Language |
| Application                              | l <b>bm</b> | <a href="#">Websphere Commerce</a> | 6.0.0.0  | All            | All     | All      |
| Application                              | l <b>bm</b> | <a href="#">Websphere Commerce</a> | 6.0.0.1  | All            | All     | All      |
| Application                              | l <b>bm</b> | <a href="#">Websphere Commerce</a> | 6.0.0.10 | All            | All     | All      |
| Application                              | l <b>bm</b> | <a href="#">Websphere Commerce</a> | 6.0.0.11 | All            | All     | All      |
| Application                              | l <b>bm</b> | <a href="#">Websphere Commerce</a> | 6.0.0.2  | All            | All     | All      |
| Application                              | l <b>bm</b> | <a href="#">Websphere Commerce</a> | 6.0.0.3  | All            | All     | All      |
| Application                              | l <b>bm</b> | <a href="#">Websphere Commerce</a> | 6.0.0.4  | All            | All     | All      |
| Application                              | l <b>bm</b> | <a href="#">Websphere Commerce</a> | 6.0.0.5  | All            | All     | All      |
| Application                              | l <b>bm</b> | <a href="#">Websphere Commerce</a> | 6.0.0.6  | All            | All     | All      |
| Application                              | l <b>bm</b> | <a href="#">Websphere Commerce</a> | 6.0.0.7  | All            | All     | All      |
| Application                              | l <b>bm</b> | <a href="#">Websphere Commerce</a> | 6.0.0.8  | All            | All     | All      |
| Application                              | l <b>bm</b> | <a href="#">Websphere Commerce</a> | 6.0.0.9  | All            | All     | All      |
| Application                              | l <b>bm</b> | <a href="#">Websphere Commerce</a> | 7.0      | All            | All     | All      |
| Application                              | l <b>bm</b> | <a href="#">Websphere Commerce</a> | 7.0      | feature_pack_8 | All     | All      |
| Application                              | l <b>bm</b> | <a href="#">Websphere Commerce</a> | 7.0.0.1  | All            | All     | All      |
| Application                              | l <b>bm</b> | <a href="#">Websphere Commerce</a> | 7.0.0.2  | All            | All     | All      |
| Application                              | l <b>bm</b> | <a href="#">Websphere Commerce</a> | 7.0.0.3  | All            | All     | All      |
| Application                              | l <b>bm</b> | <a href="#">Websphere Commerce</a> | 7.0.0.4  | All            | All     | All      |
| Application                              | l <b>bm</b> | <a href="#">Websphere Commerce</a> | 7.0.0.5  | All            | All     | All      |
| Application                              | l <b>bm</b> | <a href="#">Websphere Commerce</a> | 7.0.0.6  | All            | All     | All      |
| Application                              | l <b>bm</b> | <a href="#">Websphere Commerce</a> | 7.0.0.7  | All            | All     | All      |
| Application                              | l <b>bm</b> | <a href="#">Websphere Commerce</a> | 7.0.0.8  | All            | All     | All      |

|                                                      |     |                    |          |                |     |     |
|------------------------------------------------------|-----|--------------------|----------|----------------|-----|-----|
| Application                                          | Ibm | Websphere Commerce | 7.0.0.9  | 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      | feature_pack_8 | 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 |
| cpe:2.3:a:ibm:websphere_commerce:6.0.0.0:*:*:*:*:*:  |     |                    |          |                |     |     |
| cpe:2.3:a:ibm:websphere_commerce:6.0.0.1:*:*:*:*:*:  |     |                    |          |                |     |     |
| cpe:2.3:a:ibm:websphere_commerce:6.0.0.10:*:*:*:*:*: |     |                    |          |                |     |     |
| cpe:2.3:a:ibm:websphere_commerce:6.0.0.11:*:*:*:*:*: |     |                    |          |                |     |     |
| cpe:2.3:a:ibm:websphere_commerce:6.0.0.2:*:*:*:*:*:  |     |                    |          |                |     |     |
| cpe:2.3:a:ibm:websphere_commerce:6.0.0.3:*:*:*:*:*:  |     |                    |          |                |     |     |
| cpe:2.3:a:ibm:websphere_commerce:6.0.0.4:*:*:*:*:*:  |     |                    |          |                |     |     |
| cpe:2.3:a:ibm:websphere_commerce:6.0.0.5:*:*:*:*:*:  |     |                    |          |                |     |     |
| cpe:2.3:a:ibm:websphere_commerce:6.0.0.6:*:*:*:*:*:  |     |                    |          |                |     |     |

```
cpe:2.3:a:ibm:websphere_commerce:6.0.0.7:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:websphere_commerce:6.0.0.8:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:websphere_commerce:6.0.0.9:*:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:websphere_commerce:7.0:*:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:websphere_commerce:7.0:feature_pack_8:*:*:*:*:
```

```
cpe:2.3:a:ibm:websphere_commerce:7.0.0.1:*:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:websphere_commerce:7.0.0.2:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:websphere_commerce:7.0.0.3:*:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:websphere_commerce:7.0.0.4:*:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:websphere_commerce:7.0.0.5:*:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:websphere_commerce:7.0.0.6:*:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:websphere_commerce:7.0.0.7:*:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:websphere_commerce:7.0.0.8:*:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:websphere_commerce:7.0.0.9:*:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:websphere_commerce:6.0.0.0:*:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:websphere_commerce:6.0.0.1:*:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:websphere_commerce:6.0.0.10:*:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:websphere_commerce:6.0.0.11:::*:*:*:*:*:
```

```
cpe:2.3:a:ibm:websphere_commerce:6.0.0.2:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:websphere_commerce:6.0.0.3:*:*:*:*:*.*
```

```
cpe:2.3:a:ibm:websphere_commerce:6.0.0.4:*:*:*:*:*.*
```

```
cpe:2.3:a:ibm:websphere_commerce:6.0.0.5:*:*:*:*:*:*
```

```
cpe:2.3:a:ibm:websphere_commerce:6.0.0.6:*:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:websphere_commerce:6.0.0.7:*:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:websphere_commerce:6.0.0.8:*:*:*:*:*:*
```

```
cpe:2.3:a:ibm:websphere_commerce:6.0.0.9:*:*:*:*:*:*
```

```
cpe:2.3:a:ibm:websphere_commerce:7.0:*:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:websphere_commerce:7.0:feature_pack_8:*:*:*:*:*:
```

```
cpe:2.3:a:ibm:websphere commerce:7.0.0.1:*:*:*:*:*.*
```

|                                                     |          |
|-----------------------------------------------------|----------|
| cpe:2.3:a:ibm:websphere_commerce:7.0.0.2:*****:     |          |
| cpe:2.3:a:ibm:websphere_commerce:7.0.0.3:*****:     |          |
| cpe:2.3:a:ibm:websphere_commerce:7.0.0.4:*****:     |          |
| cpe:2.3:a:ibm:websphere_commerce:7.0.0.5:*****:     |          |
| cpe:2.3:a:ibm:websphere_commerce:7.0.0.6:*****:     |          |
| cpe:2.3:a:ibm:websphere_commerce:7.0.0.7:*****:     |          |
| cpe:2.3:a:ibm:websphere_commerce:7.0.0.8:*****:     |          |
| cpe:2.3:a:ibm:websphere_commerce:7.0.0.9:*****:     |          |
| No vendor comments have been submitted for this CVE |          |
| ← Previous ID                                       | Next ID→ |