



# CVE-2013-0459

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

## Summary

|                        |                                                                                                                             |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2013-0459                                                                                                               |
| <b>State</b>           | PUBLIC                                                                                                                      |
| <b>Assigner</b>        | psirt@us.ibm.com                                                                                                            |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                                |
| <b>Published</b>       | 2013-01-27 18:55:00 UTC                                                                                                     |
| <b>Updated</b>         | 2017-08-29 01:33:00 UTC                                                                                                     |
| <b>Description</b>     | Cross-site scripting (XSS) vulnerability in the Administrative console in IBM WebSphere Application Server (WAS) 6.1 before |

## Risk And Classification

### Problem Types: CWE-79

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor | Product                      | Version  | Update | Edition | Language |
|-------------|--------|------------------------------|----------|--------|---------|----------|
| 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 | 6.1.0.11 | 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 | 6.1.0.17 | All    | All     | All      |
| Application | IBM    | WebSphere Application Server | 6.1.0.19 | All    | All     | All      |
| Application | IBM    | WebSphere Application Server | 6.1.0.2  | All    | All     | All      |
| Application | IBM    | WebSphere Application Server | 6.1.0.21 | All    | All     | All      |
| Application | IBM    | WebSphere Application Server | 6.1.0.23 | All    | All     | All      |
| Application | IBM    | WebSphere Application Server | 6.1.0.25 | All    | All     | All      |
| Application | IBM    | WebSphere Application Server | 6.1.0.27 | All    | All     | All      |
| Application | IBM    | WebSphere Application Server | 6.1.0.29 | All    | All     | All      |
| Application | IBM    | WebSphere Application Server | 6.1.0.3  | All    | All     | All      |
| Application | IBM    | WebSphere Application Server | 6.1.0.31 | All    | All     | All      |

[illegible]



|             |     |                              |          |     |     |     |
|-------------|-----|------------------------------|----------|-----|-----|-----|
| Application | IBM | WebSphere Application Server | 7.0.0.25 | All | All | All |
| Application | IBM | WebSphere Application Server | 7.0.0.3  | All | All | All |
| Application | IBM | WebSphere Application Server | 7.0.0.5  | All | All | All |
| Application | IBM | WebSphere Application Server | 7.0.0.7  | All | All | All |
| Application | IBM | WebSphere Application Server | 7.0.0.9  | 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 | 8.0.0.2  | 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 | 8.5.0.0  | All | All | All |
| Application | IBM | WebSphere Application Server | 8.5.0.1  | All | All | All |

| References                                                                                                         |  |  |  |         |                                                                                 |  |
|--------------------------------------------------------------------------------------------------------------------|--|--|--|---------|---------------------------------------------------------------------------------|--|
| Reference                                                                                                          |  |  |  | Source  | Link                                                                            |  |
| IBM Security Bulletin: Security Vulnerabilities fixed in IBM WebSphere Application Server 7.0.0.27 - United States |  |  |  | CONFIRM | <a href="http://www.ibm.com">www.ibm.com</a>                                    |  |
| IBM notice: The page you requested cannot be displayed                                                             |  |  |  | AIXAPAR | <a href="http://www-01.ibm.com">www-01.ibm.com</a>                              |  |
| IBM X-Force Exchange                                                                                               |  |  |  | XF      | <a href="https://exchange.xforce.ibmcloud.com">exchange.xforce.ibmcloud.com</a> |  |
| CVE Program record                                                                                                 |  |  |  | CVE.ORG | <a href="http://www.cve.org">www.cve.org</a>                                    |  |
| NVD vulnerability detail                                                                                           |  |  |  | NVD     | <a href="http://nvd.nist.gov">nvd.nist.gov</a>                                  |  |

No vendor comments have been submitted for this CVE.

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