



CVE-2017-1756

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

| | |
|------------------------|--|
| CVE | CVE-2017-1756 |
| State | PUBLIC |
| Assigner | psirt@us.ibm.com |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2018-03-30 16:29:00 UTC |
| Updated | 2019-10-09 23:26:00 UTC |
| Description | IBM Business Process Manager 8.6 allows web pages to be stored locally which can be read by another user on the system |

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|-------------|--------|--------------------------|---------|--------|---------|----------|
| Application | ibm | Business Process Manager | 7.5.0.0 | All | All | All |
| Application | ibm | Business Process Manager | 7.5.0.0 | All | All | All |
| Application | ibm | Business Process Manager | 7.5.0.0 | All | All | All |
| Application | ibm | Business Process Manager | 7.5.0.1 | All | All | All |
| Application | ibm | Business Process Manager | 7.5.0.1 | All | All | All |
| Application | ibm | Business Process Manager | 7.5.0.1 | All | All | All |
| Application | ibm | Business Process Manager | 7.5.1.0 | All | All | All |
| Application | ibm | Business Process Manager | 7.5.1.0 | All | All | All |
| Application | ibm | Business Process Manager | 7.5.1.0 | All | All | All |
| Application | ibm | Business Process Manager | 7.5.1.1 | All | All | All |
| Application | ibm | Business Process Manager | 7.5.1.1 | All | All | All |
| Application | ibm | Business Process Manager | 7.5.1.1 | All | All | All |
| Application | ibm | Business Process Manager | 7.5.1.2 | All | All | All |
| Application | ibm | Business Process Manager | 7.5.1.2 | All | All | All |
| Application | ibm | Business Process Manager | 7.5.1.2 | All | All | All |
| Application | ibm | Business Process Manager | 8.0.0.0 | All | All | All |
| Application | ibm | Business Process Manager | 8.0.0.0 | All | All | All |

| | | | | | | |
|-------------|-----|---|---------|----------|-----|-----|
| Application | lbn | Business Process Manager | 8.5.6.1 | All | All | All |
| Application | lbn | Business Process Manager | 8.5.6.2 | All | All | All |
| Application | lbn | Business Process Manager | 8.5.6.2 | All | All | All |
| Application | lbn | Business Process Manager | 8.5.6.2 | All | All | All |
| Application | lbn | Business Process Manager | 8.5.7.0 | All | All | All |
| Application | lbn | Business Process Manager | 8.5.7.0 | All | All | All |
| Application | lbn | Business Process Manager | 8.5.7.0 | All | All | All |
| Application | lbn | Business Process Manager | 8.5.7.0 | cf201606 | All | All |
| Application | lbn | Business Process Manager | 8.5.7.0 | cf201606 | All | All |
| Application | lbn | Business Process Manager | 8.5.7.0 | cf201606 | All | All |
| Application | lbn | Business Process Manager | 8.5.7.0 | cf201609 | All | All |
| Application | lbn | Business Process Manager | 8.5.7.0 | cf201609 | All | All |
| Application | lbn | Business Process Manager | 8.5.7.0 | cf201609 | All | All |
| Application | lbn | Business Process Manager | 8.5.7.0 | cf201612 | All | All |
| Application | lbn | Business Process Manager | 8.5.7.0 | cf201612 | All | All |
| Application | lbn | Business Process Manager | 8.5.7.0 | cf201612 | All | All |
| Application | lbn | Business Process Manager | 8.5.7.0 | cf201703 | All | All |
| Application | lbn | Business Process Manager | 8.5.7.0 | cf201703 | All | All |
| Application | lbn | Business Process Manager | 8.5.7.0 | cf201703 | All | All |
| Application | lbn | Business Process Manager | 8.5.7.0 | cf201706 | All | All |
| Application | lbn | Business Process Manager | 8.5.7.0 | cf201706 | All | All |
| Application | lbn | Business Process Manager | 8.5.7.0 | cf201706 | All | All |
| Application | lbn | Business Process Manager | 8.6.0.0 | All | All | All |
| Application | lbn | Business Process Manager Enterprise Service Bus | 8.6.0.0 | All | All | All |
| Application | lbn | Business Process Manager Enterprise Service Bus | 8.6.0.0 | All | All | All |
| Application | lbn | Websphere | 7.2.0.0 | All | All | All |
| Application | lbn | Websphere | 7.2.0.1 | All | All | All |
| Application | lbn | Websphere | 7.2.0.2 | All | All | All |
| Application | lbn | Websphere | 7.2.0.3 | All | All | All |
| Application | lbn | Websphere | 7.2.0.4 | All | All | All |
| Application | lbn | Websphere | 7.2.0.5 | All | All | All |
| Application | lbn | Websphere | 7.2.0.0 | All | All | All |
| Application | lbn | Websphere | 7.2.0.1 | All | All | All |
| Application | lbn | Websphere | 7.2.0.2 | All | All | All |
| Application | lbn | Websphere | 7.2.0.3 | All | All | All |

| | | | | | | |
|-------------|---------------------|---------------------------|---------|-----|-----|-----|
| Application | Ibm | Websphere | 7.2.0.4 | All | All | All |
| Application | Ibm | Websphere | 7.2.0.5 | All | All | All |

References

Reference

IBM X-Force Exchange

IBM Business Process Manager CVE-2017-1756 Local Information Disclosure Vulnerability

IBM Security Bulletin: Potential information leakage in IBM Business Process Manager and WebSphere Lombardi Edition (CVE-2017-1756) - I

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](#)