



CVE-2016-0349

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

Summary

CVE	CVE-2016-0349
State	PUBLIC
Assigner	psirt@us.ibm.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-06-30 01:59:00 UTC
Updated	2016-11-30 03:02:00 UTC
Description	IBM Business Process Manager 8.5.6 through 8.5.6.2 and 8.5.7 before 8.5.7.CF201606 allows remote authenticated users

Risk And Classification

Problem Types: CWE-284

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	ibm	Business Process Manager	8.5.6.0	All	All	All
Application	ibm	Business Process Manager	8.5.7.0	All	All	All
Application	ibm	Business Process Manager	8.5.6.0	All	All	All
Application	ibm	Business Process Manager	8.5.7.0	All	All	All

References

Reference
JR55701: SECURITY APAR - CVE-2016-0349 - INCORRECT AUTHORIZATION FOR UPDATE OF PROCESS INSTANCE VARIABLES IN II
IBM Business Process Manager Access Control Flaw Lets Remote Authenticated Users Update Process Instance Variables on the Target Sys
Security Bulletin: Incorrect authorization for update of process instance variables in IBM Business Process Manager (CVE-2016-0349)
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](#)