CVE-2016-3056

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

Summary

CVE	CVE-2016-3056
State	PUBLISHED
Assigner	ibm
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-10-14 02:59:06 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Cross-site scripting (XSS) vulnerability in Business Space in IBM Business Process Manager 7.5 through 7.5.1.2, 8.0 throu

Risk And Classification

Primary CVSS: v3.0 5.4 MEDIUM from nvd@nist.gov

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

EPSS: 0.002410000 probability, percentile 0.473930000 (date 2026-05-17)

Problem Types: CWE-79 | n/a

Version	Source	Type	Score	Severity	Vector
3.0	nvd@nist.gov	Primary	5.4	MEDIUM	CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N
2.0	nvd@nist.gov	Primary	3.5		AV:N/AC:M/Au:S/C:N/I:P/A:N

CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

Required

Scope

Changed

Confidentiality

Low

Integrity

Low

Availability

None

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

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

Single

Confidentiality

None

Integrity

Partial

Availability

None

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

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	7.5.0.0	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	7.5.0.1	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	7.5.1.0	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	7.5.1.1	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	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	Ibm	Business Process Manager	8.0.0.0	All	All	All
Application	Ibm	Business Process Manager	8.0.0.0	All	All	All
Application	Ibm	Business Process Manager	8.0.1.0	All	All	All
Application	Ibm	Business Process Manager	8.0.1.0	All	All	All
Application	Ibm	Business Process Manager	8.0.1.0	All	All	All
Application	Ibm	Business Process Manager	8.0.1.0	All	All	All
Application	Ibm	Business Process Manager	8.0.1.1	All	All	All
Application	Ibm	Business Process Manager	8.0.1.1	All	All	All
Application	Ibm	Business Process Manager	8.0.1.1	All	All	All
Application	Ibm	Business Process Manager	8.0.1.1	All	All	All
Application	Ibm	Business Process Manager	8.0.1.2	All	All	All
Application	Ibm	Business Process Manager	8.0.1.2	All	All	All
Application	Ibm	Business Process Manager	8.0.1.2	All	All	All
Application	Ibm	Business Process Manager	8.0.1.2	All	All	All
Application	Ibm	Business Process Manager	8.0.1.3	All	All	All
Application	Ibm	Business Process Manager	8.0.1.3	All	All	All
Application	Ibm	Business Process Manager	8.0.1.3	All	All	All
Application	Ibm	Business Process Manager	8.0.1.3	All	All	All
Application	Ibm	Business Process Manager	8.5.0.0	All	All	All
Application	Ibm	Business Process Manager	8.5.0.0	All	All	All
Application	Ibm	Business Process Manager	8.5.0.0	All	All	All
Application	Ibm	Business Process Manager	8.5.0.0	All	All	All
Application	Ibm	Business Process Manager	8.5.0.1	All	All	All
Application	Ibm	Business Process Manager	8.5.0.1	All	All	All
Application	Ibm	Business Process Manager	8.5.0.1	All	All	All
Application	Ibm	Business Process Manager	8.5.0.1	All	All	All
Application	Ibm	Business Process Manager	8.5.0.2	All	All	All
Application	Ibm	Business Process Manager	8.5.0.2	All	All	All
Application	Ibm	Business Process Manager	8.5.0.2	All	All	All

Application	Ibm	Business Process Manager	8.5.0.2	All	All	All
Application	Ibm	Business Process Manager	8.5.5.0	All	All	All
Application	Ibm	Business Process Manager	8.5.5.0	All	All	All
Application	Ibm	Business Process Manager	8.5.5.0	All	All	All
Application	Ibm	Business Process Manager	8.5.5.0	All	All	All
Application	Ibm	Business Process Manager	8.5.6.0	All	All	All
Application	Ibm	Business Process Manager	8.5.6.0	All	All	All
Application	Ibm	Business Process Manager	8.5.6.0	All	All	All
Application	Ibm	Business Process Manager	8.5.6.0	All	All	All
Application	Ibm	Business Process Manager	8.5.6.2	All	All	All
Application	Ibm	Business Process Manager	8.5.6.2	All	All	All
Application	Ibm	Business Process Manager	8.5.6.2	All	All	All
Application	Ibm	Business Process Manager	8.5.6.2	All	All	All
Application	Ibm	Business Process Manager	8.5.7.0	All	All	All
Application	Ibm	Business Process Manager	8.5.7.0	All	All	All
Application	Ibm	Business Process Manager	8.5.7.0	All	All	All
Application	Ibm	Business Process Manager	8.5.7.0	All	All	All

Vendor Declared Affected Products

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

References

Reference
IBM Business Process Manager CVE-2016-3056 Unspecified HTML Injection Vulnerability
IBM JR56300: SECURITY APAR CVE-2016-3056 IBM BUSINESS PROCESS MANAGER AND IBM BUSINESS MONITOR ARE VULNERAB
IBM Security Bulletin: HTML injection vulnerability in Business Space might affect IBM Business Process Manager (CVE-2016-3056) - United
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.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**