CVE-2020-4578

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

Summary

CVE	CVE-2020-4578
State	PUBLIC
Assigner	psirt@us.ibm.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-09-10 17:15:00 UTC
Updated	2020-09-11 02:27:00 UTC
Description	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 is vulnerable to cross-site scripting. This vulnerability allows users

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Hp	Hp-ux	-	All	All	All
Operating System	Hp	Hp-ux	-	All	All	All
Operating System	Ibm	Aix	-	All	All	All
Operating System	Ibm	Aix	-	All	All	All
Operating System	Ibm	I	-	All	All	All
Operating System	Ibm	I	-	All	All	All
Application	Ibm	Websphere Application Server	All	All	All	All
Application	Ibm	Websphere Application Server	All	All	All	All
Application	Ibm	Websphere Application Server	All	All	All	All
Application	Ibm	Websphere Application Server	All	All	All	All
Operating System	Ibm	Z/os	-	All	All	All
Operating System	Ibm	Z/os	-	All	All	All
Operating System	Linux	Linux Kernel	-	All	All	All
Operating System	Linux	Linux Kernel	-	All	All	All
Operating System	Microsoft	Windows	-	All	All	All
Operating System	Microsoft	Windows	-	All	All	All
Operating System	Oracle	Solaris	-	All	All	All

Operating System	Oracle	Solaris	-	All	All	All

References

Reference	Source	Link
IBM X-Force Exchange	XF	exchang
Security Bulletin: WebSphere Application Server Admin Console is vulnerable to cross-site scripting (CVE-2020-4578)	CONFIRM	www.ibı
CVE Program record	CVE.ORG	www.cv
NVD vulnerability detail	NVD	nvd.nist

No vendor comments have been submitted for this CVE.

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