CVE-2018-1840

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

Summary

CVE	CVE-2018-1840
State	PUBLIC
Assigner	psirt@us.ibm.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-12-03 15:29:00 UTC
Updated	2019-10-09 23:39:00 UTC
Description	IBM WebSphere Application Server 8.5 and 9.0 could allow a remote attacker to gain elevated privileges on the system, ca

Risk And Classification

Problem Types: CWE-668

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ibm	Websphere Application Server	All	All	All	All
Application	Ibm	Websphere Application Server	All	All	All	All

References

Reference	Source	Link
IBM X-Force Exchange	XF	exchange.xfor
Security Bulletin: Potential Privilege escalation vulnerability in WebSphere Application Server (CVE-2018-1840)	CONFIRM	www.ibm.com
IBM WebSphere Application Server CVE-2018-1840 Remote Privilege Escalation Vulnerability	BID	www.securityfo
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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 registred 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