IBM WebSphere Application Server Liberty could provide weaker than expected security

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2025-14917
State	PUBLISHED
Assigner	ibm
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-03-25 21:16:24 UTC
Updated	2026-03-30 16:59:11 UTC
Description	IBM WebSphere Application Server - Liberty 17.0.0.3 through 26.0.0.3 IBM WebSphere Application Server Liberty could pr

Risk And Classification

Primary CVSS: v3.1 9.8 CRITICAL from nvd@nist.gov

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

EPSS: 0.000370000 probability, percentile 0.109200000 (date 2026-04-01)

Problem Types: CWE-1393 | CWE-1393 CWE-1393 Use of Default Password

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
3.1	psirt@us.ibm.com	Secondary	6.7	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	CVSS	6.7	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

ntegrity

High

Availability

High

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

NVD Known Affected Configurations (CPE 2.3)

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	IBM	WebSphere Application Server - Liberty	affected 17.0.0.3 26.0.0.3 semver	Not specified

References

Reference	Source	Link	Tags
www.ibm.com/support/pages/node/7267362	psirt@us.ibm.com	www.ibm.com	Vendor Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Solutions

CNA: IBM strongly recommends addressing the vulnerability now by applying a currently available interim fix or fix pack that contains the fix for APAR PH70078. To determine if a feature is enabled for IBM WebSphere Application Server Liberty, refer to How to determine if Liberty is using a specific feature https://www.ibm.com/support/pages/node/6553910 . Attention: After installing the interim fix or fixpack, please follow the additional instructions provided in the interim fix link referenced below to complete the remediation. For IBM WebSphere Application Server Liberty 17.0.0.3 - 26.0.0.3 using the appSecurity-1.0,

appSecurity-2.0, appSecurity-3.0, appSecurity-4.0 or appSecurity-5.0 feature(s): · Upgrade to minimal fix pack levels as required by the interim fix and then apply the Interim Fix that resolves PH70078 https://www.ibm.com/support/pages/node/7266845 and carefully follow the instructions for steps required after fix installation. --OR-- · Apply Liberty Fix Pack 26.0.0.4 or later (targeted availability 2Q2026). Additional interim fixes may be available and linked off the interim fix download page.

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