IBM WebSphere Application Server Liberty is affected by identity spoofing

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

Summary

CVE	CVE-2026-3621
State	PUBLISHED
Assigner	ibm
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-23 00:16:45 UTC
Updated	2026-04-23 00:16:45 UTC
Description	IBM WebSphere Application Server - Liberty 17.0.0.3 through 26.0.0.4 IBM WebSphere Application Server Liberty is vulner

Risk And Classification

Primary CVSS: v3.1 7.5 HIGH from psirt@us.ibm.com

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

Problem Types: CWE-269 | CWE-269 CWE-269 Improper Privilege Management

Version	Source	Type	Score	Severity	Vector
3.1	psirt@us.ibm.com	Primary	7.5	HIGH	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H
3.1	CNA	CVSS	7.5	HIGH	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H

CVSS v3.1 Breakdown

Attack Vector
Network

Attack Complexity
High

Privileges Required
Low

User Interaction
None

Scope
Unchanged

Confidentiality
High

Integrity
High

Availability

High

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

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	IBM	WebSphere Application Server - Liberty	affected 17.0.0.3 26.0.0.4 semver	Not specified

References

Reference	Source	Link	Tags
www.ibm.com/support/pages/node/7270437	psirt@us.ibm.com	www.ibm.com	
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 PH70352. IBM WebSphere Application Server Liberty is affected by identity spoofing only when the appSecurity feature (appSecurity-1.0, appSecurity-2.0, appSecurity-3.0, appSecurity-4.0, or appSecurity-5.0) is not enabled on the server. 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 . For IBM WebSphere Application Server Liberty 17.0.0.3 - 26.0.0.4: · Upgrade to minimal fix pack levels as required by the interim fix and then apply the Interim Fix that resolves PH70352 https://www.ibm.com/support/pages/node/7270436 --OR-- · Apply Liberty Fix Pack 26.0.0.5 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.

Free CVE JSON API cve.report/api

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