



Security Bulletin: IBM WebSphere Application Server Liberty is affected by identity spoofing (CVE-2026-3621)

Security Bulletin

Summary

IBM WebSphere Application Server Liberty is affected by identity spoofing 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.

Vulnerability Details

CVEID: [CVE-2026-3621](https://www.cve.org/CVERecord?id=CVE-2026-3621) (<https://www.cve.org/CVERecord?id=CVE-2026-3621>)

DESCRIPTION: IBM WebSphere Application Server Liberty is vulnerable to identity spoofing under limited conditions when an application is deployed without authentication and authorization configured.

CWE: [CWE-269: Improper Privilege Management](https://cwe.mitre.org/data/definitions/269.html) (<https://cwe.mitre.org/data/definitions/269.html>)

CVSS Source: IBM

CVSS Base score: 7.5

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

Affected Products and Versions

Affected Product(s)	Version(s)
IBM WebSphere Application Server - Liberty	17.0.0.3 - 26.0.0.4

Remediation/Fixes

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)

(<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) (<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.

Workarounds and Mitigations

None

Get Notified about Future Security Bulletins

 Subscribe to [My Notifications](https://www.ibm.com/support/pages/node/718119) (<https://www.ibm.com/support/pages/node/718119>) to be notified of important product support alerts like this.

References

[Complete CVSS v3 Guide](#) 

[On-line Calculator v3](#) 

Related Information

[IBM Secure Engineering Web Portal](http://www.ibm.com/security/secure-engineering/bulletins.html) (<http://www.ibm.com/security/secure-engineering/bulletins.html>)

[IBM Product Security Incident Response Blog](http://www.ibm.com/blogs/psirt) (<http://www.ibm.com/blogs/psirt>)

Acknowledgement

Change History

22 Apr 2026: Initial Publication

*The CVSS Environment Score is customer environment specific and will ultimately impact the Overall CVSS Score. Customers can evaluate the impact of this vulnerability in their environments by accessing the links in the Reference section of this Security Bulletin.

Disclaimer

According to the Forum of Incident Response and Security Teams (FIRST), the Common Vulnerability Scoring System (CVSS) is an "industry open standard designed to convey vulnerability severity and help to determine urgency and priority of response." IBM PROVIDES THE CVSS SCORES ""AS IS"" WITHOUT WARRANTY OF ANY KIND, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. CUSTOMERS ARE RESPONSIBLE FOR ASSESSING THE IMPACT OF ANY ACTUAL OR POTENTIAL SECURITY VULNERABILITY. In addition to other efforts to address potential vulnerabilities, IBM periodically updates the record of components contained in our product offerings. As part of that effort, if IBM identifies previously unidentified packages in a product/service inventory, we address relevant vulnerabilities regardless of CVE date. Inclusion of an older CVEID does not demonstrate that the referenced product has been used by IBM since that date, nor that IBM was aware of a vulnerability as of that date. We are making clients aware of relevant vulnerabilities as we become aware of them. "Affected Products and Versions" referenced in IBM Security Bulletins are intended to be only products and versions that are supported by IBM

and have not passed their end-of-support or warranty date. Thus, failure to reference unsupported or extended-support products and versions in this Security Bulletin does not constitute a determination by IBM that they are unaffected by the vulnerability. Reference to one or more unsupported versions in this Security Bulletin shall not create an obligation for IBM to provide fixes for any unsupported or extended-support products or versions.

Document Information

More support for:

[WebSphere Application Server](https://www.ibm.com/mysupport/s/topic/0TO50000001DQQGA2) (<https://www.ibm.com/mysupport/s/topic/0TO50000001DQQGA2>)

Software version:

Liberty

Operating system(s):

AIX, IBM i, Linux, Windows, z/OS, Mac OS

Document number:

7270437

Modified date:

22 April 2026

Initial Publish date:

22 April 2026