



TLP: CLEAR

CALIFORNIA CYBERSECURITY INTEGRATION CENTER



## CYBER ADVISORY

Tuesday, June 02, 2026

CAL-CSIC-202606-A-001

### Spoofing Vulnerability Impacting IBM WebSphere Application Server

Spoofing

Unauthorized Access

CIA Compromise

Interim Patch Available

The Cybersecurity Integration Center (CSIC) has identified a critical-severity spoofing vulnerability impacting multiple versions of IBM's WebSphere Application Server. CVE-2026-8644 carries a CVSS 3.1 score of 9.1.<sup>1</sup> The vulnerability enables an unauthenticated attacker to impersonate users or system components, leading to unauthorized access and/or manipulation of data. Successful exploitation compromises the confidentiality, integrity, and availability of applications running on a compromised server.<sup>2</sup>

The attack can be initiated remotely over the network, as impersonate legitimate entities over the network once credentials or identity tokens are presented to the server. No Proof-of-Concept (PoC) is publicly available at this time, nor is it considered to be a zero-day exploit. CVE-2026-8644 has no confirmed exploitation in the wild.

IBM has issued an interim fix pack that contains the fix for CVE-2026-8644. There are no workarounds for this vulnerability.

The Cal-CSIC recommends following IBM's guidance to download and install the IBM interim fix (APAR PH71422), then perform application and identity-verification tests to confirm that the spoofed credential attempts are rejected and that legitimate authentication continues to function as intended.

For additional technical vulnerability details and IBM's security bulletin for CVE-2026-8644, please use this link:

<https://www.ibm.com/support/pages/node/7274740>

**WARNING:** This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for **TLP: CLEAR**, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.

**TLP: CLEAR**

## Affected Product(s) and Version(s)

| Product                          | Version                   |
|----------------------------------|---------------------------|
| IBM WebSphere Application Server | V9.0.0.0 through 9.0.5.28 |
|                                  | V8.5.0.0 through 8.5.5.29 |

Cal-CSIC services are provided at no cost to assist organizations in strengthening their cybersecurity defenses. If you need assistance or wish to verify this communication, please contact us at (833) REPORT-1, or (916) 636-2997. Visit our website for more details: [California Cybersecurity Integration Center | California Governor's Office of Emergency Services](#)

---

## References

---

<sup>1</sup> OpenCVE; “CVE-2026-8466”; <https://app.openCVE.io/cve/CVE-2026-8644>; accessed 02 June 2026

<sup>2</sup> IBM; “Security Bulletin: IBM WebSphere Application Server is affected by an identity spoofing vulnerability (CVE-2026-8644)”; <https://www.ibm.com/support/pages/node/7274740>; accessed 02 June 2026

**WARNING:** This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for **TLP: CLEAR**, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.

**TLP: CLEAR**