مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerabilities in IBM WebSphere Application Server

Tracking #:432319089

Date:08-06-2026

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed multiple critical vulnerabilities in IBM WebSphere Application Server that could allow unauthorized access and remote code execution. Successful exploitation may lead to system compromise and service disruption.

TECHNICAL DETAILS:

Vulnerability Details

- **CVE-2026-8644**
  - Severity: Critical | CVSS: 9.1
  - An authentication bypass vulnerability that could allow identity spoofing and unauthorized access to affected systems.
- **CVE-2026-9319**
  - Severity: Critical | CVSS: 9.0
  - A deserialization vulnerability in JAX-WS endpoints with WS-Security that could enable remote code execution.
- **CVE-2026-9311**
  - Severity: Critical | CVSS: 9.0
  - A remote code execution vulnerability caused by the bypass of security controls.
- **CVE-2026-9330**
  - Severity: High | CVSS: 8.5
  - An improper validation vulnerability in the SAML SSO component that could lead to remote code execution through crafted requests.

Affected Products

- IBM WebSphere Application Server – Versions 9.0.0.0 through 9.0.5.28
- IBM WebSphere Application Server – Versions 8.5.0.0 through 8.5.5.29

Fixed Versions and Mitigations

For WebSphere Application Server 9.0

- Apply the Interim Fixes addressing APARs PH71422, PH71453, and PH71454 after upgrading to the required minimum fix pack level.
- Alternatively, upgrade to **Fix Pack 9.0.5.29** or later when available.

For WebSphere Application Server 8.5

- Apply the Interim Fixes addressing APARs PH71422, PH71453, and PH71454 after upgrading to the required minimum fix pack level.
- Alternatively, upgrade to **Fix Pack 8.5.5.30** or later when available.

RECOMMENDATIONS:

- Identify affected IBM WebSphere Application Server deployments.
- Apply the available interim fixes for APARs PH71422, PH71453, and PH71454 without delay.
- Upgrade to the latest supported fix packs as soon as they become available.
- Prioritize remediation of internet-facing and critical systems.
- Review security configurations and minimize unnecessary exposure of services.
- Monitor systems and logs for suspicious or unauthorized activity.
- Verify that remediation measures have been successfully implemented.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://www.ibm.com/support/pages/node/7274733
- https://www.ibm.com/support/pages/node/7274738
- https://www.ibm.com/support/pages/node/7274740