



مجلس الأمن السيبراني  
CYBER SECURITY COUNCIL



**Multiple Vulnerabilities in IBM WebSphere Application Server**

Tracking #:432319248

Date:06-07-2026

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLIGENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

## EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed IBM has released a security bulletin addressing multiple vulnerabilities affecting IBM WebSphere Application Server.

## TECHNICAL DETAILS:

IBM has released a security bulletin addressing multiple vulnerabilities affecting IBM WebSphere Application Server versions 9.0 and 8.5. The vulnerabilities include two critical Cross-Site Scripting (XSS) flaws and one Path Traversal vulnerability that could allow attackers to execute malicious scripts in the administrative console or access sensitive information from the integrated help system.

### Vulnerability Details:

#### 1. CVE: CVE-2026-11712

Severity: **Critical**

CVSS Score: 9.3

Type: Cross-Site Scripting (XSS)

CWE: CWE-79

Description: An XSS vulnerability in the administrative console help system could allow attackers to execute malicious scripts in an administrator's browser.

#### 2. CVE: CVE-2026-11708

Severity: Critical

CVSS Score: 9.3

Type: Cross-Site Scripting (XSS)

CWE: CWE-79

Description: An XSS vulnerability in the administrative console integrated help system could allow execution of malicious scripts and compromise administrator sessions.

#### 3. CVE: CVE-2026-11595

Severity: Medium

CVSS Score: 4.3

Type: Path Traversal

CWE: CWE-22

Description: A path traversal vulnerability could allow remote attackers to access sensitive information from the administrative console's integrated help system.

### Affected Products:

Product	Affected Versions
IBM WebSphere Application Server	9.0
IBM WebSphere Application Server	8.5

### Fixed Version:

#### For IBM WebSphere Application Server 9.0

- Upgrade to the minimum required Fix Pack level and apply the Interim Fix for APAR PH71756.
- OR
- Upgrade to Fix Pack 9.0.5.29 or later (targeted availability: Q3 2026).

### For IBM WebSphere Application Server 8.5

- Upgrade to the minimum required Fix Pack level and apply the Interim Fix for APAR PH71756.
- OR
- Upgrade to Fix Pack 8.5.5.31 or later (targeted availability: Q3 2026).

## RECOMMENDATIONS:

### Immediate Actions:

- Apply the Interim Fix or upgrade to the latest IBM WebSphere Application Server Fix Pack.

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/7278590>