مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerability in MICS REST API Server

Tracking #:432318839

Date:24-04-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical security vulnerability has been identified in the MICS Resource Management REST API Server component (MBAS), impacting environments running on z/OS.

TECHNICAL DETAILS:

A critical security vulnerability (CVSS 9.1) has been identified in the MICS Resource Management 14.5 – REST API Server component (MBAS), impacting environments running on z/OS. The flaw, tracked as CVE-2026-22732, arises from a vulnerable implementation within Spring Security.

Vulnerability Details

- CVE ID: CVE-2026-22732
- Severity: CRITICAL (9.1)
- Vendor: Broadcom
- Product: MICS Resource Management
- Affected Version: 14.5 (MICS REST API Server only)
- Unaffected Versions: 14.3, 14.4
- Affected Component: MBAS (MICS REST API Server)
- Root Cause: Vulnerability in Spring Security (version upgrade from 5.8.21 → 5.8.24)
- Solution: PTF LU20158

Key Risk Characteristics:

- Remotely exploitable over network
- No authentication required (PR:N)
- No user interaction required (UI:N)
- Low attack complexity (AC:L)
- No privilege escalation required

RECOMMENDATIONS:

Immediate Actions:

- Apply the vendor-provided patch.

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://support.broadcom.com/web/ecx/support-content-notification/-/external/content/securityadvisories/0/37391/