

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Critical Remote Code Execution in ServiceNow AI Platform

Tracking #:432318468

Date:27-02-2026

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 that a critical vulnerability, CVE-2026-0542, has been identified in the ServiceNow AI Platform, allowing unauthenticated remote code execution (RCE) within the platform's AI Sandbox.

TECHNICAL DETAILS:

A critical vulnerability, CVE-2026-0542, has been identified in the ServiceNow AI Platform, allowing unauthenticated remote code execution (RCE) within the platform's AI Sandbox.

Vulnerability Details

- **CVE ID:** CVE-2026-0542
- **Severity:** Critical (CVSSv4: 9.2)
- **Affected Component:** ServiceNow AI Platform – Sandbox environment
- **Type:** Remote Code Execution (RCE)

RECOMMENDATIONS:

Immediate Action:

- Verify instance version and ensure the latest security patches are applied.
- If environment is hosted, confirm that instance received the January 2026 security update.

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.servicenow.com/kb?id=kb_article_view&sysparm_article=KB2693566