

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Critical Privilege Escalation in ServiceNow AI Platform
Tracking #:432318254
Date:15-01-2026

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 ServiceNow addressed a critical privilege escalation vulnerability (CVE-2025-12420) in its AI Platform.

TECHNICAL DETAILS:

ServiceNow addressed a critical privilege escalation vulnerability (CVE-2025-12420) in its AI Platform that could have allowed an unauthenticated attacker to impersonate legitimate users and perform actions with their privileges by exploiting flawed account-linking and authentication logic, potentially bypassing MFA and SSO controls.

Vulnerability Details:

- Vulnerability ID: CVE-2025-12420
- Severity: Critical
- CVSS Score: 9.8 (ServiceNow rating)
- Vulnerability Class: Execution with Unnecessary Privileges (CWE-250)
- Affected Platform: ServiceNow AI Platform
- Affected Components:
 - Now Assist AI Agents
 - Virtual Agent API

Affected Products and Fixed Versions

Now Assist AI Agents (sn_aia)

- **Fixed in:**
 - Version **5.1.18** or later
 - Version **5.2.19** or later

Virtual Agent API (sn_va_as_service)

- **Fixed in:**
 - Version **3.15.2** or later
 - Version **4.0.4** or later

RECOMMENDATIONS:

- Verify deployed versions of Now Assist AI Agents and Virtual Agent API and Apply updates immediately if running vulnerable versions

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=KB2587329