Critical ServiceNow Vulnerabilities Allow Code Execution and SQL Injection

Author: *Portia S. Cole – CTI Researcher*

TL;DR

ServiceNow patched three critical AI Platform vulnerabilities: CVE-2026-18885, CVE-2026-18886 and CVE-2026-74820, each with a CVSS score of 10.0. The flaws could allow unauthenticated code execution, privilege escalation or SQL injection.

ServiceNow also fixed CVE-2026-6876, a high-severity Now Platform sandbox escape with a CVSS score of 8.7. ServiceNow updated hosted instances, provided patches to partners and self-hosted customers, and reports no malicious exploitation.

Overview

There are three critical vulnerabilities in the ServiceNow AI Platform. The vulnerabilities, tracked as CVE-2026-18885, CVE-2026-18886 and CVE-2026-74820, each have a CVSS score of 10.0. They can be exploited remotely without authentication or user interaction. ServiceNow also fixed a high-severity Now Platform sandbox escape, tracked as CVE-2026-6876 with a CVSS score of 8.7.

ServiceNow AI Platform is used to manage IT services, automate workflows and connect business systems. Organizations may use ServiceNow to handle support tickets, employee requests, security operations, asset data, customer service and other business processes.

An attacker who exploits these flaws may be able to view or change data in the affected ServiceNow instance and interfere with the workflows it supports. Depending on how the instance is configured, the code execution and SQL injection vulnerabilities may also put its database and connected systems at risk.

ServiceNow said it deployed security updates to hosted instances and provided the updates to partners and self-hosted customers. Customers enrolled in the ServiceNow Patching Program received the updates automatically. ServiceNow is not aware of malicious exploitation, and no public exploit code has been identified at this time.

Self-hosted customers must apply the appropriate update or upgrade. Hosted customers should verify that their instance received the security update and is running a fixed release.

Published on: 8/28/2026

Vulnerability Breakdown

- **CVE-2026-18885** (CVSS 10.0) - A code injection vulnerability in the GraphQL Composite Data API could allow an unauthenticated attacker, under certain circumstances, to execute arbitrary code and access or modify instance data.

- **CVE-2026-18886** (CVSS 10.0) - Improper access control in the system configuration image upload processor could allow an unauthenticated attacker to create or modify instance data and escalate privileges.

- **CVE-2026-74820** (CVSS 10.0) - A SQL injection vulnerability involving a dynamic schema ORDER BY clause could allow an unauthenticated attacker to execute SQL statements against the instance database and access or modify data.

- **CVE-2026-6876** (CVSS 8.7) - A sandbox escape could allow arbitrary code execution within the Now Platform and provide more access than intended. ServiceNow describes the issue as unauthenticated, although its CVSS vector lists low privileges as required.

Affected Versions

ServiceNow lists the following fixed releases. Versions earlier than the applicable release on each branch are affected:

- Xanadu: Patch 11 Hot Fix 7a
- Yokohama: Patch 12 Hot Fix 3b or Patch 13 Hot Fix 4
- Zurich: Patch 7b Hot Fix 3, Patch 8 Hot Fix 5, Patch 9 Hot Fix 6, Patch 10 Hot Fix 2m for the m-branch, Patch 10 Hot Fix 3 for the standard branch, Patch 11 or Patch 12
- Australia: Patch 2 Hot Fix 3, Patch 3 Hot Fix 2, Patch 3m, Patch 4 or Patch 5

Impact on Aspire Customers

Aspire customers may rely on ServiceNow to manage IT support and automate business processes.

A compromised instance could expose ServiceNow records and credentials used by integrations. An attacker could also change permissions or interfere with workflows that support other business operations.

The greatest immediate risk is to unpatched self-hosted and partner-hosted instances, particularly those accessible from the Internet. ServiceNow-hosted customers should still verify that the update was applied to their instance.

The Common Vulnerability Scoring System (CVSS) rates vulnerabilities from 0 to 10 based on exploitability and potential impact.

- None (0.0): No severity
- Low (0.1–3.9): Limited impact
- Medium (4.0–6.9): Moderate risk
- High (7.0–8.9): Serious impact
- Critical (9.0–10.0): Severe impact requiring urgent attention

Aspire Protects

- **Patch** - Apply the appropriate fixed release immediately to self-hosted and partner-hosted instances. See ServiceNow's security advisories for further details.
  - CVE-2026-18885
  - CVE-2026-18886
  - CVE-2026-74820
  - CVE-2026-6876
- For ServiceNow-hosted instances, verify that the security update was applied and compare the current patch level with the fixed releases in the ServiceNow advisory.
- Review instance audit logs and history for unexpected unauthenticated requests, code execution, SQL activity, data or configuration changes, and new or modified privileged accounts and roles.
- Review credentials and tokens used by ServiceNow integrations if suspicious activity is found. Rotate any credentials that may have been exposed.

TTPs to Watch

Initial Access

- Exploit Public-Facing Application [T1190]: An attacker may send crafted requests to an Internet-accessible ServiceNow instance to exploit the code injection, access control or SQL injection vulnerabilities.

Privilege Escalation

- Account Manipulation [T1098]: Successful exploitation could allow an attacker to create or modify instance data and gain elevated access. Monitor for unexpected changes to accounts, groups, roles and permissions.

Impact

- Data Manipulation [T1565]: An attacker could use SQL injection or unauthorized instance access to alter records, configurations or workflow data.

IoCs

There are no known IoCs at this time. Aspire is actively monitoring and will notify customers if any are found. For more details on how we can help protect your organization, contact Aspire's Customer Success Management team.

Targeted Industries

ServiceNow is used across the public and private sectors, including:

- Public Sector
- Education
- Healthcare
- Finance
- Legal & Professional Services
- Retail
- Manufacturing
- Energy

Aspire Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors.
  - Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyber attacks.
- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will

ultimately maintain business continuity, protect the company's reputation, and avoid fines, legal fees, and remediation costs.
    - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

- **NOC Services Notice**
    - If you are an Aspire NOC customer and are affected by these vulnerabilities, Aspire will open a case on your behalf. Customers interested in NOC services should contact Aspire's Customer Success Management team.

Supporting Documentation

August 2026 CVE Advisory Notification - Security

Landing Page | ServiceNow Common Vulnerabilities & Exposures (CVE) Security Advisories - Security

CVE Record: CVE-2026-18885

CVE Record: CVE-2026-74820

CVE Record: CVE-2026-6876