

Critical ServiceNow AI Platform Vulnerabilities Could Expose Instance Data

Author: Portia S. Cole – CTI Researcher

Overview

ServiceNow released fixes for five vulnerabilities (CVE-2026-13016, CVE-2026-86860, CVE-2026-86858, CVE-2026-86859, and CVE-2026-86857) affecting its AI Platform. Four can be exploited without an account. The remaining vulnerability requires access to an authenticated user account.

The two critical vulnerabilities involve SQL injection and missing authorization. They could allow someone without credentials to access the underlying database or extract information from an affected ServiceNow instance. The other vulnerabilities could expose records or allow instance data to be changed or deleted.

ServiceNow says customers participating in its August Patching Program received the appropriate update. Self-hosted customers must install a fixed release if they have not already done so.

Vulnerability Breakdown

CVE-2026-13016 (CVSS 9.3)

- An unauthenticated attacker could send SQL commands to the database behind an affected ServiceNow instance. This could provide access to stored information or allow the attacker to change instance data.

CVE-2026-86860 (CVSS 9.3)

- A missing authorization check could allow an unauthenticated attacker to extract instance data and gain additional privileges.

Other Vulnerabilities

- **CVE-2026-86858** (CVSS 8.7): An unauthenticated attacker could create, change, or delete instance data.
- **CVE-2026-86859** (CVSS 8.7): An unauthenticated attacker could access data they are not permitted to view.

TL;DR

There are five high and critical vulnerabilities in ServiceNow AI Platform (CVE-2026-13016, CVE-2026-86860, CVE-2026-86858, CVE-2026-86859, and CVE-2026-86857).

An attacker could access, change, delete, or extract instance data, depending on the vulnerability. ServiceNow has not reported exploitation.

- **CVE-2026-86857** (CVSS 8.4): An authenticated user could access data outside their assigned permissions and potentially gain further access.

Affected Products

ServiceNow AI Platform releases earlier than the following fixed versions are affected:

- Yokohama Patch 13 Hot Fix 5a
- Zurich Patch 10 Hot Fix 3b
- Zurich Patch 10 Hot Fix 4a W32
- Zurich Patch 11 Hot Fix 3
- Australia Patch 2 Hot Fix 4b W32
- Australia Patch 4 Hot Fix 3
- Australia Patch 5

Yokohama, Zurich, and Australia are ServiceNow release names, not geographic locations.

Impact on Aspire Customers

Someone without a ServiceNow account could access or alter information stored in an affected instance. Depending on how ServiceNow is used, this may include support tickets, employee requests, asset records, security cases, or configuration details.

Changes to records or workflows could also interfere with IT operations and delay work handled through the platform.

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** - Confirm the ServiceNow release and patch level for each instance. See ServiceNow's [security advisory](#) for more information.

- Upgrade self-hosted instances to a fixed release.
- Confirm hosted instances received the September security update.

TTPs to Watch

Initial Access

- Exploit Public-Facing Application [T1190]: An attacker could send crafted requests to an affected ServiceNow instance to exploit the SQL injection or access-control vulnerabilities without signing in. (CVE-2026-13016, CVE-2026-86858, CVE-2026-86859, CVE-2026-86860)

Collection

- Data from Information Repositories [T1213]: An attacker could access or extract records stored in the ServiceNow instance. (CVE-2026-13016, CVE-2026-86857, CVE-2026-86859, CVE-2026-86860)

Impact

- Data Manipulation [T1565]: An attacker could create, change, or delete instance data. (CVE-2026-13016, CVE-2026-86858)

Privilege Escalation

- Exploitation for Privilege Escalation [T1068]: An attacker could exploit the missing authorization flaw to gain access beyond the permissions normally allowed. (CVE-2026-86860)

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

These vulnerabilities impact organizations that use ServiceNow AI Platform to manage enterprise workflows or store operational and customer data.

- Public Sector
- Finance
- Healthcare
- Manufacturing
- Energy
- Education

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 any vulnerability in this notice, Aspire will open a case on your behalf. Customers interested in NOC services should contact Aspire's Customer Success Management team.

Supporting Documentation

[\[Security Advisory\] September 2026 CVE Advisory Notification - Security](#)