



CYBER ADVISORY

Thursday, October 01, 2026

CAL-CSIC-202610-A-002

Multiple Vulnerabilities Impacting ServiceNow AI Platform

Unauthorized Access

Data Modification

Arbitrary SQL Code Execution

Fixed Releases Available

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of multiple high and critical rated vulnerabilities discovered in ServiceNow's AI Platform, one of which would allow for unauthorized access. The ServiceNow AI Platform is used to integrate AI, data, and workflow automation to execute business operations across the enterprise infrastructure.¹

The following vulnerabilities were discovered:

- [CVE-2026-13016](#): SQL injection vulnerability allowing unauthenticated users to execute arbitrary SQL statements (CVSS v4.0: 9.3)²
- [CVE-2026-86860](#): Missing authorization enabling unauthenticated users to extract data and escalate privileges (CVSS v4.0: 9.3)³
- [CVE-2026-86858](#): Improper access control, enabling unauthenticated users to modify/delete data (CVSS v4.0: 8.7)⁴
- [CVE-2026-86859](#): Authorization bypass for unauthenticated users to access unauthorized data (CVSS v4.0: 8.7)⁵
- [CVE-2026-86857](#): Authorization bypass in ServiceNow AI Platform, allowing authenticated users to access unauthorized data (CVSS v4.0: 8.4)⁶

Among these, CVE-2026-13016 is one the most impactful. The vulnerability stems from insufficient input validation. An attacker would be able to send crafted requests to the platform in order to execute arbitrary SQL code against the underlying database and gain access to or modify instance data beyond what was intended.

ServiceNow identified the vulnerabilities through internal security testing, customer security assessments, and various disclosure and bug bounty programs. ServiceNow has not identified any confirmed evidence of exploitation. and have issued a security advisory with software updates to address this vulnerability. ServiceNow has also stated that they have remediated these vulnerabilities.⁷

The Cal-CSIC recommends that any self-hosted clients follow ServiceNow's updating guidance and upgrade to their appropriate patched release. Customers who participate in the ServiceNow Patching Program have received an update.

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for **TLP: CLEAR**, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.

For additional details regarding these ServiceNow vulnerabilities, please use this link:

ServiceNow Security Advisory:

https://support.servicenow.com/kb?id=kb_article_view&sysparm_article=KB3159623

Affected Release and Updated Versions

ServiceNow AI Platform Release	Updated Version
Yokohama	Patch 13 Hot Fix 5a
Zurich	Patch 10 Hot Fix 4a W32 Patch 10 Hot Fix 3b Patch 11 Hot Fix 3
Australia	Patch 2 Hot Fix 4b W32 Patch 4 Hot Fix 3 Patch 5

Cal-CSIC services are provided at no cost to assist organizations in strengthening their cybersecurity defenses. If you need assistance or wish to verify this communication, please contact us at (833) REPORT-1, or (916) 636-2997. Visit our website for more details: [California Cybersecurity Integration Center | California Governor's Office of Emergency Services](#)

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for **TLP: CLEAR**, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.

TLP: CLEAR

References

- ¹ CIS; "Multiple Vulnerabilities in ServiceNow's AI Platform Could Allow for Unauthorized Access"; https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-servicenows-ai-platform-could-allow-for-unauthorized-access_2026-102; accessed 01 October 1, 2026
- ² OpenCVE; "CVE-2026-13016"; <https://app.opencve.io/cve/CVE-2026-13016>; accessed 01 October 1, 2026
- ³ OpenCVE; "CVE-2026-86860"; <https://app.opencve.io/cve/CVE-2026-86860>; accessed 01 October 1, 2026
- ⁴ OpenCVE; "CVE-2026-86858"; <https://app.opencve.io/cve/CVE-2026-86858>; accessed 01 October 1, 2026
- ⁵ OpenCVE; "CVE-2026-86859"; <https://app.opencve.io/cve/CVE-2026-86859>; accessed 01 October 1, 2026
- ⁶ OpenCVE; "CVE-2026-86857"; <https://app.opencve.io/cve/CVE-2026-86857>; accessed 01 October 1, 2026
- ⁷ ServiceNow; "Security Advisory September 2026 CVE Advisory Notification"; https://support.servicenow.com/kb?id=kb_article_view&sysparm_article=KB3159623; accessed 01 October 1, 2026

WARNING: This document is the property of the California Cybersecurity Integration Center (CAL-CSIC) and follows Traffic Light Protocol (TLP) standards. Except for **TLP: CLEAR**, all TLP designations require recipients to control, store, handle, transmit, and dispose of this product accordingly. Do not release to the public, media, or unauthorized personnel without prior CAL-CSIC approval. This document may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 7920.000 et seq.). CAL-CSIC does not guarantee the completeness or accuracy of the information.

TLP: CLEAR