

Alert Bulletin

Bulletin N.: 93

Publication Date: 28/08/2026

Subject: Alert 2026-93 Critical Vulnerabilities in ServiceNow AI Platform

Traffic Light Protocol (TLP): White

Affected product(s):

The three CVEs affect **ServiceNow AI Platform**. Instances running versions prior to the following patches within their release family must be updated:

- **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 (*m* branch), Patch 10 Hot Fix 3 (standard), Patch 11 or Patch 12.
- **Australia:** Patch 2 Hot Fix 3, Patch 3 Hot Fix 2, Patch 3m, Patch 4 or Patch 5.

Description

ServiceNow reported and fixed three critical vulnerabilities in **ServiceNow AI Platform**, a PaaS platform aimed at automating business workflows and integrating AI capabilities. Public records do not attribute the discovery of the three flaws to an individual researcher. All of them have **CVSS v4.0: 10.0 (Critical)**, are remotely exploitable with low complexity, require no authentication or user interaction, and may compromise confidentiality, integrity, and availability of the instance.

CVE-2026-18885 is a code injection flaw in the **GraphQL Composite Data** API. Under certain circumstances, an unauthenticated attacker could execute arbitrary code within the platform and access or modify instance data beyond intended permissions.

CVE-2026-18886 is an improper access control vulnerability in the configuration image upload processor. Its exploitation would allow an unauthenticated user to create or modify instance data and, as a consequence, escalate privileges.

CVE-2026-74820 is a SQL injection linked to an ORDER BY clause with dynamic schema. An unauthenticated attacker could execute arbitrary SQL statements against the underlying database of the instance, with the ability to read or alter information outside the authorized scope.

ServiceNow indicated that it has already deployed the security updates on instances hosted by the company and distributed the patches to partners and self-hosted customers. At the time of publication, there was no knowledge of malicious exploitation of these three vulnerabilities.

Solution:

Self-hosted customers should urgently apply the corresponding *hot fix* or patch for their version family, or upgrade to a patched version. Customers with ServiceNow-managed instances should confirm that the update has already been applied to each instance, including development, testing, and contingency environments.

The patch and version-specific instructions are available in the official ServiceNow advisory: [KB3152242](#).

As a complementary measure, it is recommended to restrict external exposure of non-essential APIs and functions, review anomalous access and unauthorized changes in administrative logs, and retain audit logs for API, GraphQL, authentication, and database activity. Because the three flaws allow unauthenticated attacks, they must be treated as the highest remediation priority.

Additional information:

- https://support.servicenow.com/kb?id=kb_article_view&sysparm_article=KB3152242
- <https://digital.nhs.uk/cyber-alerts/2026/cc-4839>

<https://www.bleepingcomputer.com/news/security/servicenow-warns-of-three-max-severity-security-vulnerabilities>