Boletín de alerta

Boletín Nro.: 93
Fecha de publicación: 28/08/2026
Tema: Alerta 2026-93 Vulnerabilidades críticas en ServiceNow AI Platform
Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

Las tres CVE afectan a **ServiceNow AI Platform**. Deben actualizarse las instancias que utilicen versiones anteriores a los siguientes parches de su familia de lanzamiento:

- **Xanadu:** Patch 11 Hot Fix 7a.
- **Yokohama:** Patch 12 Hot Fix 3b o 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 (rama *m*), Patch 10 Hot Fix 3 (estándar), Patch 11 o Patch 12.
- **Australia:** Patch 2 Hot Fix 3, Patch 3 Hot Fix 2, Patch 3m, Patch 4 o Patch 5.

Descripción

ServiceNow reportó y corrigió tres vulnerabilidades críticas en **ServiceNow AI Platform**, plataforma PaaS orientada a automatizar flujos empresariales e integrar capacidades de IA. Los registros públicos no atribuyen el descubrimiento de las tres fallas a un investigador individual. Todas cuentan con **CVSS v4.0: 10.0 (Crítica)**, son explotables remotamente con baja complejidad, sin autenticación ni interacción de usuario, y pueden comprometer confidencialidad, integridad y disponibilidad de la instancia.

CVE-2026-18885 es una inyección de código en la API **GraphQL Composite Data**. Bajo determinadas circunstancias, un atacante no autenticado podría ejecutar código arbitrario dentro de la plataforma y acceder a datos de la instancia o modificarlos fuera de los permisos previstos.

CVE-2026-18886 es una vulnerabilidad de control de acceso inadecuado en el procesador de carga de imágenes de configuración del sistema. Su explotación permitiría a un usuario no autenticado crear o modificar datos de la instancia y, como consecuencia, escalar privilegios.

CVE-2026-74820 es una inyección SQL vinculada a una cláusula ORDER BY con esquema dinámico. Un atacante no autenticado podría ejecutar sentencias SQL arbitrarias contra la base de datos subyacente de la instancia, con capacidad de leer o alterar información fuera del alcance autorizado.

ServiceNow indicó que ya desplegó las actualizaciones de seguridad en las instancias hospedadas por la compañía y distribuyó los parches para socios y clientes autohospedados. Al momento de la publicación, no se tenía conocimiento de explotación maliciosa de estas tres vulnerabilidades.

Solución:

Los clientes autohospedados deben aplicar con urgencia el *hot fix* o parche correspondiente a su familia de versión, o actualizar a una versión corregida. Los clientes con instancias gestionadas por ServiceNow deben confirmar que la actualización ya se haya aplicado a cada instancia, incluidos los ambientes de desarrollo, pruebas y contingencia.

El parche y las instrucciones específicas por versión se encuentran en el aviso oficial de ServiceNow: **KB3152242.**

Como medida complementaria, se recomienda restringir la exposición externa de APIs y funciones no esenciales, revisar accesos anómalos y cambios no autorizados en registros administrativos, y conservar los registros de auditoría de API, GraphQL, autenticación y actividad de base de datos. Debido a que las tres fallas permiten ataques sin autenticación, deben tratarse como prioridad máxima de remediación.

Información adicional:

- **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