Boletín de alerta

Boletín Nro.: 63
Fecha de publicación: 11/06/2026
Tema: Alerta 2026-63 Vulnerabilidad Crítica en ServiceNow
Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

El fabricante acota el alcance a instancias que ejecutan la platform release “Australia” y a instancias en releases anteriores donde se aplicaron ciertas configuraciones que dejaban expuesto el endpoint REST vulnerable.

Descripción

Se ha publicado recientemente una vulnerabilidad sin CVE público en **ServiceNow** que habría permitido a un usuario no autenticado ganar mayor acceso al previsto sobre determinadas instancias de clientes y consultar datos almacenados en tablas internas de la plataforma. ServiceNow detectó actividad anómala relacionada con este problema, confirmó consultas exitosas contra un subconjunto de clientes y desplegó un parche en sus instancias hospedadas el 5 de junio de 2026.

Aunque los primeros reportes hablaron de una explotación activa por actores desconocidos, posteriormente la compañía indicó que la evidencia observada apuntaría, por ahora, a **investigadores de seguridad y equipos de investigación de clientes** vinculados a programas de bug bounty, y no a actores maliciosos confirmados. Aun así, desde una perspectiva defensiva, cualquier acceso no autenticado exitoso a tablas de instancia debe tratarse como un incidente de **alta severidad**, especialmente por la naturaleza sensible de la información alojada en ServiceNow en entornos corporativos.

La falla habría estado relacionada con un **endpoint API expuesto sin autenticación** en determinadas condiciones, permitiendo que solicitudes HTTP no autenticadas consultaran información de instancias afectadas. Los análisis públicos más repetidos apuntan al endpoint /api/now/related_list_edit/create y a una configuración equivalente a requires_authentication=false, aunque ese detalle técnico no ha sido confirmado públicamente por ServiceNow en un advisory abierto.

Desde el punto de vista operativo, esto implica que no era necesario comprometer credenciales ni explotar una cadena compleja: bastaba con identificar una instancia afectada y abusar del endpoint vulnerable para obtener acceso no deseado a datos de la instancia. ServiceNow indicó que la actividad comenzó el **2 de junio de 2026**, que entre el 3 y 4 de junio recibió reportes vía bug bounty, y que el 5 de junio aplicó el fix

en sus entornos hospedados.

Mitigación

Para clientes de ServiceNow, la primera medida es **confirmar con el proveedor** si la instancia estaba dentro del subconjunto afectado y si ya recibió la actualización aplicada el 5 de junio. También conviene revisar si la organización está sobre la release **Australia** o si hizo cambios de configuración en versiones anteriores que pudieran haber ampliado la exposición.

A nivel defensivo, es recomendable:

- Revisar logs HTTP y de API buscando accesos anómalos o no autenticados al endpoint señalado públicamente.
- Buscar consultas inusuales a tablas de instancia durante la ventana del 2 al 5 de junio de 2026.
- Correlacionar indicadores como la IP 51.159.98.241, compartida públicamente por defensores como posible IOC de acceso externo.
- Tratar cualquier evidencia de consulta no autorizada como posible exposición de datos y activar respuesta a incidente orientada a revisión de tablas, auditoría de accesos y notificación interna.

Solución

En instancias **hosted**, la solución principal fue aplicada por ServiceNow mediante un **security update** desplegado el 5 de junio de 2026. La acción inmediata para clientes no es instalar manualmente un parche clásico, sino validar con ServiceNow que su instancia fue corregida y que no quedaron configuraciones personalizadas que mantengan exposición equivalente.

Como medidas complementarias, conviene revisar:

- Endpoints personalizados o integraciones expuestas sin autenticación.
- Registros de acceso y exportaciones de datos en la ventana afectada.
- Reglas de monitoreo para detectar consultas anómalas a tablas sensibles.

Información adicional:

- SecurityWeek – ServiceNow Patches Vulnerability Exploited Against Some Customers
- The Hacker News – ServiceNow Flaw Exploited to Gain Unauthorized Access to Customer Instances
- TechCrunch – ServiceNow tells customers a bug left some of their data exposed to the internet
- National CIO Review – ServiceNow Responds to Security Issue After Unauthorized Activity
- BleepingComputer – ServiceNow discloses security incident exposing customer data