

CONFIDENCIAL · PAGO

EJEMPLO FICTICIO

EXPEDIENTE · TARUMA-PAGOS

Taruma Pagos. Informe técnico

VENTANA	2026-09-01 a 2026-09-30
ALCANCE	6 activos autorizados
HALLAZGOS	1 crítica · 1 alta · 4 medias · 2 bajas · 2 informativas
ORIGEN	Empresa ficticia. Hallazgos basados en auditorías reales.



01 · RESUMEN DE RIESGO

Hallazgos confirmados

10 hallazgos confirmados: 1 crítica, 1 alta, 4 medias, 2 bajas, 2 informativas.

PANORAMA DE RIESGO

Hallazgos por dominio y severidad

	CRÍTICA	ALTA	MEDIA	BAJA	INFO	TOTAL
Web	1	1	1	2	1	6
Smart contract	.	.	1	.	.	1
Servidor	.	.	.	.	1	1
Red	.	.	1	.	.	1
Móvil	.	.	1	.	.	1
TOTAL	1	1	4	2	2	10

ID	ACTIVO	DOMINIO	SEVERIDAD	PUNTAJE	ESTADO
web-sso-01	app-web	Web	CRÍTICA	9 . 1	Confirmado
web-cache-04	app-web	Web	ALTA	7 . 4	Confirmado
web-race-02	app-web	Web	MEDIA	6 . 5	Confirmado
net-subdomain-06	dns-taruma	Red	MEDIA	6 . 1	Confirmado
mob-key-08	app-movil	Móvil	MEDIA	5 . 3	Confirmado
sc-sig-03	settlement-contract	Smart contract	MEDIA	Impacto alto, probabilidad baja	Confirmado
web-dep-07	api-graphql	Web	BAJA	3 . 7	Confirmado

ID	ACTIVO	DOMINIO	SEVERIDAD	PUNTAJE	ESTADO
web-ssrf-05	api-graphql	Web	BAJA	3.1	Confirmado
net-tls-10	api-legacy	Servidor	INFO	0.0	Confirmado
web-graphql-09	api-graphql	Web	INFO	0.0	Confirmado

02 · DETALLE TÉCNICO

Hallazgos completos

web-sso-01

El inicio de sesión con Microsoft permite a una organización ajena entrar como administrador de una empresa cliente

CVSS 3.1

9.1**CRÍTICA**

PROFUNDIDAD

INFO

BAJA

MEDIA

ALTA

CRÍTICA

ID

web-sso-01

VECTOR

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

ACTIVO

app-web

DOMINIO

Web

ESTADO

Confirmado

DESCRIPCIÓN

El inicio de sesión federado con Microsoft identifica al usuario por la dirección de correo que viene en el token y no por el identificador estable de la cuenta y su organización de origen. Como la dirección de correo la controla quien administra la organización de origen, una organización ajena puede presentar un token legítimo con el correo de un administrador de Tarumá, y la aplicación lo acepta como ese administrador. El vínculo entre la cuenta externa y la cuenta interna se hace por un dato que el atacante elige, no por uno que Tarumá controla.

IMPACTO EN EL NEGOCIO

Un atacante entra como administrador de la empresa cliente cuyo correo conozca, sin su contraseña ni su segundo factor. Desde ahí aprueba lotes de pago, cambia las cuentas bancarias de destino y ve los datos de todos los proveedores de esa empresa. Es el camino directo al movimiento de fondos y a los datos personales, y no deja rastro de un acceso forzado porque el inicio de sesión es, en apariencia, legítimo.

EXPOSICIÓN ECONÓMICA

USD 250k a 3M

Suma los fondos desviados de lotes aprobados en nombre de una empresa cliente, la filtración de los datos bancarios de sus proveedores, el costo de respuesta y la demora de la ronda. El extremo bajo supone detección antes de la liquidación; el alto, fondos ya liquidados.

EXPOSICIÓN LEGAL Y REGULATORIA

Ley 25.326 (Argentina), art. 9, deber de seguridad

Ley 19.670 art. 38 y Decreto 64/020 (Uruguay), aviso en 72 horas

LGPD y Res. CD/ANPD 15/2024 (Brasil), aviso en 3 días hábiles

El acceso a datos bancarios y de identidad de proveedores es un incidente sobre datos personales. Uruguay: aviso a la URCDP en 72 horas. Brasil: aviso a la ANPD y a los afectados en 3 días hábiles si hay riesgo relevante. Argentina: compromete el deber de seguridad; notificar a la AAIP se recomienda.

Orientativo: no constituye asesoramiento legal.

EVIDENCIA

poc/ingreso.md

```
sha256:79b84512190de5cf4208613eb8d3189c805469fba5796c0c  
c5a19527a5c69f93
```

Ingreso como administrador de prueba desde una identidad externa; el control con la cuenta verificada es rechazado

PRUEBA DE CONCEPTO

Se demostró el acceso como un administrador de prueba de Tarumá desde una organización de identidad que nosotros controlábamos, sin usar ninguna credencial de la víctima. Como control, el mismo flujo con el identificador estable y la organización de origen verificados rechaza la entrada, lo que aísla que la falla está en confiar en el correo y no en la verificación de la cuenta.

CORRECCIÓN

Vincular la cuenta por el identificador estable del usuario y el identificador de su organización de origen, no por el correo, y rechazar la entrada de organizaciones que no estén en una lista autorizada. No usar el correo ni el nombre de usuario como identificador: en Microsoft esos datos no prueban que la organización de origen sea dueña del dominio. Para los clientes ya dados de alta, re-vincular las cuentas contra el identificador estable en la próxima sesión.

REVISIÓN ADVERSARIAL

Veredicto **confirmado** frente a web-bounty OWASP (A07 fallas de identificación y autenticación; patrón de confianza en el correo del token).

- acceso propio (descartado: el ingreso se logró con una identidad externa, no la de la víctima)
- correo verificado que coincide por azar (descartado: el correo era elegido por el atacante)

web-cache-04

La página de claves de API de un cliente queda guardada en la caché pública y la ve un anónimo

CVSS 3.1

7.4**ALTA****PROFUNDIDAD**

INFO

BAJA

MEDIA

ALTA

CRÍTICA

ID

web-cache-04

VECTOR

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:N/A:N

ACTIVO

app-web

DOMINIO

Web

ESTADO

Confirmado

DESCRIPCIÓN

La red de distribución de contenido decide que guardar en su caché pública mirando la extensión del final de la dirección, antes de que la aplicación decida si esa página es privada. Pidiendo la página privada de claves de API con una extensión de archivo estático agregada al final, la respuesta, que contiene datos de la sesión de la víctima, queda guardada en la caché y luego se sirve a cualquiera que pida esa misma dirección. Es el patrón conocido como engaño de caché web.

IMPACTO EN EL NEGOCIO

Un atacante que logra que la víctima visite un enlace preparado deja la página privada de esa víctima guardada en la caché pública, y después la recupera sin estar autenticado. Expone las claves de API de la empresa cliente, que permiten operar contra la plataforma en su nombre.

EXPOSICIÓN ECONÓMICA**USD 30k a 200k**

La exposición son las claves de API de las empresas clientes cuyos administradores abran el enlace, y lo que se pueda operar con ellas hasta su rotación. Escala con la cantidad de víctimas alcanzadas, no es una filtración masiva en un solo paso.

EXPOSICIÓN LEGAL Y REGULATORIA

Ley 25.326 (Argentina), art. 9, deber de seguridad

Ley 19.670 art. 38 y Decreto 64/020 (Uruguay), aviso en 72 horas

LGPD y Res. CD/ANPD 15/2024 (Brasil), aviso en 3 días hábiles

La exposición de credenciales y de datos de la cuenta de un cliente compromete el deber de seguridad sobre datos personales. Si se confirma acceso efectivo a datos de personas, en Uruguay hay que avisar a la URCDP en 72 horas y en Brasil a la ANPD en 3 días hábiles si hay riesgo relevante; en Argentina, la AAIP recomienda notificar.

Orientativo: no constituye asesoramiento legal.

EVIDENCIA

`poc/cache.md`

```
sha256:1fc65b727a7bbf85e34fe5e123bcfedf232fe54ddff46b4876707334634fb2c1
```

La respuesta privada queda en la caché y se recupera sin sesión; la dirección normal no se cachea

PRUEBA DE CONCEPTO

Se demostró, sobre una cuenta de prueba propia, que la respuesta privada queda almacenada en la caché y se recupera después sin sesión. El control con la dirección normal, sin la extensión agregada, no se almacena. No se usó ninguna cuenta de cliente real.

CORRECCIÓN

Hacer que la decisión de cachear dependa de las cabeceras que envía la aplicación y no de la extensión de la dirección; marcar como no cacheable toda respuesta autenticada. En la red de distribución, no cachear por extensión rutas que pueden ser dinámicas. Rotar las claves de API que pudieran haber quedado expuestas.

REVISIÓN ADVERSARIAL

Veredicto **confirmado** frente a web-bounty (engaño de caché web; interacción entre la CDN y la autorización de la app).

- contenido público (descartado: la página afectada requiere sesión y muestra datos del titular)
- caché local del navegador (descartado: la respuesta se recuperó desde otra red sin sesión)

web-race-02

Se puede superar el límite diario de pagos enviando varias órdenes en simultáneo

CVSS 3.1

6.5

MEDIA

PROFUNDIDAD

INFO	
BAJA	
MEDIA	
ALTA	
CRÍTICA	

ID

web-race-02

VECTOR

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N

ACTIVO

app-web

DOMINIO

Web

ESTADO

Confirmado

DESCRIPCIÓN

El control del límite diario de pagos lee el total acumulado, decide y luego lo actualiza, sin tratar esos pasos como una sola operación indivisible. Cuando varias órdenes llegan juntas, todas leen el mismo total anterior y todas pasan el control antes de que alguna lo actualice, de modo que el límite se supera. Es una condición de carrera clásica en el camino de aprobación de pagos.

IMPACTO EN EL NEGOCIO

Un usuario con permiso para iniciar pagos, pero sujeto a un tope diario, puede ordenar pagos por mucho más que ese tope en un mismo momento. El tope existe justamente para contener el error y el fraude interno; sin él, una cuenta comprometida o un empleado desleal mueve montos muy por encima de lo previsto antes de que nadie lo note.

EXPOSICIÓN ECONÓMICA

USD 80k a 600k

La pérdida es el exceso que se mueve por encima del tope antes de la detección, acotado por el saldo disponible de la cuenta y la ventana hasta la liquidación. La banda toma topes diarios típicos y la cantidad de órdenes que entran en una sola ráfaga.

EVIDENCIA

poc/limite.md

sha256:225fe2b5c79867ed4f2cb8b513d3ce474f69356d0b4250f1b72afc87d4e661bc

Varias órdenes simultáneas cuyo total excede el tope se aprueban; el envío secuencial respeta el tope

PRUEBA DE CONCEPTO

Se demostró que un conjunto de órdenes enviadas a la vez, cuyo total supera el tope diario, se aprueban todas, mientras que enviadas una tras otra la segunda es rechazada. El control una-tras-otra confirma que el problema es la simultaneidad y no el cálculo del tope.

CORRECCIÓN

Aplicar el límite dentro de una transacción que bloquee el registro del acumulado (o un bloqueo por cuenta), de modo que las órdenes concurrentes se evalúen en serie. Agregar una verificación final antes de liquidar y una prueba que lance varias órdenes a la vez y espere que solo pasen las que caben en el tope.

REVISIÓN ADVERSARIAL

Veredicto **confirmado** frente a web-bounty OWASP (condición de carrera en límites; patrón TOCTOU en aprobación de pagos).

- doble envío accidental (descartado: cada orden era distinta y válida)
- tope mal configurado (descartado: el envío secuencial respeta el tope correctamente)

net-subdomain-06

Un subdominio apunta a un servicio dado de baja y puede ser reclamado por un tercero

CVSS 3.1

6.1**MEDIA**

PROFUNDIDAD

INFO	
BAJA	
MEDIA	
ALTA	
CRÍTICA	

ID

net-subdomain-06

VECTOR

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

ACTIVO

dns-taruma

DOMINIO

Red

ESTADO

Confirmado

DESCRIPCIÓN

El subdominio de la página de estado del servicio sigue apuntando, por DNS, a una plataforma externa donde el recurso ya fue dado de baja. Mientras ese registro siga publicado, un tercero puede dar de alta el recurso en esa plataforma y quedarse con el subdominio, sirviendo contenido bajo el nombre de Tarumá.

IMPACTO EN EL NEGOCIO

Quien reclame el subdominio puede publicar páginas que parecen oficiales de Tarumá, útil para engañar a clientes o empleados y para campañas de phishing con un dominio legítimo. Daña la confianza en la marca y facilita el robo de credenciales.

EXPOSICIÓN ECONÓMICA

USD 10k a 90k

El costo es reputacional y de respuesta ante un uso del subdominio para engañar a clientes; no hay pérdida directa de fondos. La banda refleja el alcance de una campaña de phishing con un dominio legítimo.

EVIDENCIA

poc/subdominio.md

sha256:6899e3ebc8c130e54d55fb5cda8df8a7533e766736b18686019610eace5ae371

El subdominio resuelve a una plataforma externa donde el recurso fue dado de baja y puede reclamarse

PRUEBA DE CONCEPTO

Se verificó que el subdominio resuelve a una plataforma externa donde el recurso no existe y que la plataforma permite reclamarlo. Por las reglas del trabajo NO se reclamó: solo se confirmó la condición y se dejó la evidencia.

CORRECCIÓN

Eliminar el registro DNS que quedó colgado, o volver a tomar el recurso en la plataforma externa. Revisar el resto de los subdominios en busca de registros hacia servicios dados de baja e incluir esa revisión en el monitoreo continuo.

REVISIÓN ADVERSARIAL

Veredicto **confirmado** frente a OSINT / superficie (subdominio reclamable; verificado sin reclamar, por las reglas del trabajo).

- servicio activo (descartado: el recurso no existe en la plataforma de destino)
- subdominio sin uso (descartado: resuelve públicamente y es alcanzable)

mob-key-08

La app móvil incluye una clave de API de un servicio de mapas sin restricción de uso

CVSS 3.1

5.3**MEDIA**

PROFUNDIDAD

INFO	
BAJA	
MEDIA	
ALTA	
CRÍTICA	

ID

mob-key-08

VECTOR

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L

ACTIVO

app-movil

DOMINIO

Móvil

ESTADO

Confirmado

DESCRIPCIÓN

El paquete público de la app móvil contiene una clave de API de un servicio de mapas. Cualquiera que inspeccione el paquete la obtiene. La clave no tiene restricción por aplicación ni por dominio, así que se puede usar desde afuera de la app, lo que consume la cuota pagada de Tarumá.

IMPACTO EN EL NEGOCIO

El riesgo es el consumo de la cuota del servicio de mapas a costa de Tarumá, con un costo económico acotado. No da acceso a datos de clientes ni a fondos. Se verificó el alcance de la clave sin usarla para generar cargos.

EVIDENCIA

poc/clave_movil.md

```
sha256:208eb939639cc2556449f0893313ca649901b6c3f223250601e4e4ebcd30e7a5
```

La clave está en el paquete público y el servicio la acepta desde fuera de la app

PRUEBA DE CONCEPTO

Se identificó la clave en el paquete público y se confirmó, con una consulta de prueba sin costo hecha desde fuera de la app, que el servicio la acepta sin restricción de origen. No se realizaron consultas que generaran cargos.

CORRECCIÓN

Restringir la clave por aplicación y por los servicios que realmente usa; rotarla; mantener las claves de terceros fuera del paquete cuando el servicio lo permita. Revisar el resto del paquete en busca de otros secretos.

REVISIÓN ADVERSARIAL

Veredicto **confirmado** frente a escaneo de secretos del paquete móvil (alcance verificado sin generar cargos).

- clave de ejemplo (descartado: es la clave de producción del servicio de mapas)
- clave ya restringida (descartado: el servicio la acepta desde fuera de la app)

sc-sig-03

Una orden firmada en el entorno de pruebas se puede ejecutar en producción

IMPACTO x PROBABILIDAD

MEDIA

IMPACTO

Alto

PROBABILIDAD

Baja

PROFUNDIDAD

INFO

BAJA

MEDIA

ALTA

CRÍTICA

ID

sc-sig-03

ACTIVO

settlement-contract

DOMINIO

Smart contract

ESTADO

Confirmado

DESCRIPCIÓN

Las órdenes de liquidación se autorizan con una firma sobre datos estructurados. El dominio de esa firma no incluye la dirección del contrato que la va a ejecutar, y los contratos de pruebas y de producción comparten el mismo firmante en la misma red. En consecuencia una firma emitida para una orden de pruebas es también válida para el contrato de producción: no queda atada al contrato para el que se creó.

IMPACTO EN EL NEGOCIO

Una orden pensada para el entorno de pruebas, donde los montos y las contrapartes no son reales, puede reutilizarse para ordenar una liquidación real en producción. Rompe la separación entre probar y operar, que es una de las garantías que un banco socio y un auditor esperan encontrar.

EXPOSICIÓN ECONÓMICA

USD 50k a 400k

El riesgo es la ejecución en producción de órdenes que nunca se pensaron como reales. La banda toma el tamaño típico de una orden de liquidación y la cantidad de firmas de prueba en circulación; no hay pérdida de capital custodiado fuera de esas órdenes.

EVIDENCIA

poc/firma.md

```
sha256:2b419a151e0a1b674e3012cf584e183318b304441ef4918d867c33a7cd5a5abc
```

Una orden firmada para el contrato de pruebas es aceptada por el de producción; con el dominio atado al contrato se rechaza

PRUEBA DE CONCEPTO

Se verificó, con revisión del código del contrato en el commit fijado y una prueba sobre una copia de la red, que una orden firmada para el contrato de pruebas es aceptada por el de producción. El control con el dominio de firma atado a la dirección del contrato hace que la misma firma sea rechazada.

CORRECCIÓN

Incluir la dirección del contrato y el identificador de la red en el dominio de la firma, de modo que cada firma sea válida solo para el contrato y la red para los que se creó. Usar firmantes distintos para pruebas y producción. Revisar si hay órdenes firmadas previas que debieran invalidarse.

REVISIÓN ADVERSARIAL

Veredicto **confirmado** frente a sc-bounty (reutilización de firma por dominio incompleto; separación de entornos).

- firma reutilizable por diseño (descartado: no hay un caso de uso que lo requiera)
- mismo contrato en ambos entornos (descartado: son despliegues distintos con la misma clave)

03 · SEVERIDAD MENOR

Bajas e informativas

BAJA CVSS 3.7 web-dep-07 api-graphql · Web

Una librería con una vulnerabilidad publicada está presente, pero la función afectada no se usa

DESCRIPCIÓN

El análisis automático de dependencias marcó como alta una librería con una vulnerabilidad publicada. El análisis de alcanzabilidad muestra que la función vulnerable no es llamada desde el código de Tarumá por ningún camino: la ruta que sería necesaria para explotarla no existe en esta aplicación. Por eso se informa como baja, no como alta: el riesgo real es mantenimiento, no una vía de ataque activa hoy.

IMPACTO EN EL NEGOCIO

Hoy no hay un camino de explotación, así que el riesgo inmediato es bajo. Importa igual porque un cambio futuro del código podría empezar a usar la función afectada, y porque conviene no arrastrar dependencias con vulnerabilidades conocidas.

EVIDENCIA

`poc/dependencia.md`

`sha256:7fdb1e901c6bc2c4a18944e964db48f711efdb7e5e6dd4930d1194ab07709359`

La función vulnerable no es alcanzable desde el código en el commit fijado

PRUEBA DE CONCEPTO

Se revisó, sobre el código en el commit fijado, que la función vulnerable no se invoca por ningún camino alcanzable. Se deja constancia de la versión instalada y de la ruta ausente.

CORRECCIÓN

Actualizar la librería a una versión corregida en el próximo ciclo de mantenimiento. Mantener el análisis de alcanzabilidad en el proceso para no tratar toda alerta del escáner como crítica ni descartarla sin revisar.

REVISIÓN ADVERSARIAL

Veredicto **confirmado** frente a SCA + análisis de alcanzabilidad (severidad ajustada de alta a baja por impacto real).

- falso positivo del escáner (descartado: la librería y la versión existen)
- función vulnerable en uso (descartado por el análisis de alcanzabilidad)

BAJA CVSS 3.1 web-ssrf-05 api-graphql · Web

El validador de webhooks se puede dirigir a la red interna, con alcance limitado

DESCRIPCIÓN

Al dar de alta un webhook, la plataforma consulta la dirección indicada para validarla. Un nombre de dominio bajo control del atacante puede resolver primero a una dirección externa (para pasar la validación) y luego a una dirección interna (cuando la plataforma hace la consulta real), técnica conocida como reenlazado de DNS. Así la consulta sale hacia la red interna. Importante: el servicio de metadatos de la nube exige el método endurecido (IMDSv2), que está activo, por lo que NO se pudieron obtener credenciales de la nube; el alcance se limita a confirmar que se alcanzan servicios internos.

IMPACTO EN EL NEGOCIO

Un atacante autenticado puede hacer que la plataforma consulte servicios de la red interna que no deberían ser alcanzables desde afuera. En esta instalación el impacto está contenido porque las credenciales de la nube están protegidas; sigue siendo un punto de apoyo hacia adentro que, combinado con otra debilidad interna, podría crecer. Se informa como baja, no crítica, justamente porque el robo de credenciales quedó bloqueado.

EXPOSICIÓN ECONÓMICA

USD 15k a 120k

El impacto directo es el acceso a servicios internos de bajo valor; la banda refleja un riesgo de apoyo, no una filtración confirmada, dado que el camino a credenciales está cerrado. El extremo alto supone encadenar con otra debilidad interna.

EVIDENCIA

`poc/webhook.md`

`sha256:6994745f10858afc08cd7f269a7e501e653da04cbcf8c1f32c5491656641644c`

La consulta de validación alcanza un servicio interno; el acceso al servicio de metadatos es rechazado

PRUEBA DE CONCEPTO

Se confirmó que una dirección bajo nuestro control reenlazada a una dirección interna hace que la plataforma la consulte, y que el intento de alcanzar el servicio de metadatos de la nube es rechazado por el método endurecido. El control con una dirección que resuelve siempre a una externa se comporta como se espera.

CORRECCIÓN

Resolver el nombre una sola vez y validar esa misma dirección que luego se consulta (evitar que cambie entre la validación y el uso); rechazar direcciones de rangos internos y de enlace local; hacer las consultas de webhook desde una red sin acceso a servicios internos. Mantener IMDSv2 obligatorio.

REVISIÓN ADVERSARIAL

Veredicto **confirmado** frente a web-bounty (SSRF por reenlazado de DNS; verificación de impacto contra el servicio de metadatos).

- destino legítimo mal clasificado (descartado: la dirección final era de un rango interno)
- acceso a credenciales de la nube (descartado y verificado: IMDSv2 lo bloquea)

INFO

CVSS 0.0 net-tls-10 api-legacy · Servidor

Un host de API heredado todavía acepta una versión de TLS obsoleta

DESCRIPCIÓN

El host de la API heredada acepta TLS 1.0, una versión del protocolo de cifrado considerada obsoleta y retirada de los requisitos de la industria. No se observó tráfico sensible activo por ese host, por lo que el riesgo real es de cumplimiento y de higiene, no una exposición directa hoy.

IMPACTO EN EL NEGOCIO

Mantener una versión obsoleta del cifrado es un hallazgo típico de los cuestionarios de cumplimiento y de los pedidos de un banco socio. El riesgo práctico es bajo mientras no circule información sensible por ese host, pero conviene cerrarlo antes de una auditoría formal.

EVIDENCIA

poc/tls.md

sha256:1ba53d90348571db8172e0ef2d81c53b9a41d61788c6c3b0bf94671ae2f8ac26

El host negocia TLS 1.0 además de las versiones vigentes

PRUEBA DE CONCEPTO

Se verificó con una prueba de la configuración de cifrado que el host negocia TLS 1.0, además de las versiones vigentes.

CORRECCIÓN

Deshabilitar TLS 1.0 y 1.1 y dejar solo TLS 1.2 y 1.3 en el host heredado. Incluir la postura de cifrado en el monitoreo continuo para detectar regresiones.

REVISIÓN ADVERSARIAL

Veredicto **confirmado** frente a infraestructura / TLS (versión de protocolo obsoleta en un host heredado).

- host sin uso (descartado: responde y negocia la conexión)

INFO

CVSS 0.0 web-graphql-09 api-graphql · Web

La API GraphQL expone su esquema completo en producción (introspección activa)

DESCRIPCIÓN

La consulta de introspección está habilitada en producción, de modo que cualquiera obtiene el esquema completo de la API: todos los tipos, campos y operaciones, incluidos los que no se usan desde la aplicación. No es una falla por sí misma, pero le entrega a un atacante el mapa de la API y facilita encontrar operaciones poco protegidas.

IMPACTO EN EL NEGOCIO

Baja el esfuerzo de reconocimiento de un atacante: en lugar de adivinar, lee el mapa de la API. Es información útil para quien busque debilidades, sin ser por sí sola una vía de acceso.

EVIDENCIA

`poc/introspeccion.md`

`sha256:1bdbb5c262c6328a01a84d6a31d975599aa8d342ef8cb452091b0740782ed30f`

La consulta de introspección devuelve el esquema completo en producción

PRUEBA DE CONCEPTO

Se obtuvo el esquema completo con una consulta de introspección contra el entorno de producción.

CORRECCIÓN

Deshabilitar la introspección en producción y dejarla solo en entornos de desarrollo. Revisar que las operaciones sensibles tengan su propia autorización, sin depender de que el esquema sea poco conocido.

REVISIÓN ADVERSARIAL

Veredicto **confirmado** frente a superficie de ataque (introspección de GraphQL en producción).

- entorno de desarrollo (descartado: la consulta fue contra producción)

INFORME TÉCNICO

Preparado para Taruma Pagos.

Este informe trae la reproducción y la corrección de cada hallazgo confirmado, más una nueva verificación dentro de la ventana del trabajo. Si quieres asesoramiento legal sobre estas obligaciones, podemos ponerte en contacto con abogados especializados.