

CONFIDENCIAL · PAGO

EJEMPLO FICTICIO

EXPEDIENTE · TARUMA-PAGOS

Taruma Pagos.

Resumen ejecutivo

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 · EL RIESGO DE UN VISTAZO

Qué está en juego

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

ATENCIÓN INMEDIATA

Confirmamos 1 vulnerabilidad crítica con una prueba que funciona: El inicio de sesión con Microsoft permite a una organización ajena entrar como administrador de una empresa cliente. El informe técnico trae la reproducción y la corrección. Hay que actuar hoy: escríbenos a security@lop.run.

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

HALLAZGO	ÁREA	SEVERIDAD	PUNTAJE
El inicio de sesión con Microsoft permite a una organización ajena entrar como administrador de una empresa cliente	app-web	CRÍTICA	9.1
La página de claves de API de un cliente queda guardada en la caché pública y la ve un anónimo	app-web	ALTA	7.4
Se puede superar el límite diario de pagos enviando varias órdenes en simultáneo	app-web	MEDIA	6.5
Un subdominio apunta a un servicio dado de baja y puede ser reclamado por un tercero	dns-taruma	MEDIA	6.1

HALLAZGO	ÁREA	SEVERIDAD	PUNTAJE
La app móvil incluye una clave de API de un servicio de mapas sin restricción de uso	app-movil	MEDIA	5.3
Una orden firmada en el entorno de pruebas se puede ejecutar en producción	settlement-contract	MEDIA	Impacto alto, probabilidad baja
Una librería con una vulnerabilidad publicada está presente, pero la función afectada no se usa	api-graphql	BAJA	3.7
El validador de webhooks se puede dirigir a la red interna, con alcance limitado	api-graphql	BAJA	3.1
Un host de API heredado todavía acepta una versión de TLS obsoleta	api-legacy	INFO	0.0
La API GraphQL expone su esquema completo en producción (introspección activa)	api-graphql	INFO	0.0

02 · EN TÉRMINOS DE NEGOCIO

Los hallazgos para la dirección

Hallazgo 1 de 10

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

ÁREA

app-web

DOMINIO

Web

QUÉ ESTÁ EN JUEGO

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.

Hallazgo 2 de 10

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

ÁREA

app-web

DOMINIO

Web

QUÉ ESTÁ EN JUEGO

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.

Hallazgo 3 de 10

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

CVSS 3.1

6.5

MEDIA

PROFUNDIDAD



ÁREA

app-web

DOMINIO

Web

QUÉ ESTÁ EN JUEGO

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.

Hallazgo 4 de 10

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

CVSS 3.1

6.1**MEDIA**

PROFUNDIDAD



ÁREA

dns-taruma

DOMINIO

Red

QUÉ ESTÁ EN JUEGO

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.

Hallazgo 5 de 10

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

CVSS 3.1

5.3**MEDIA**

QUÉ ESTÁ EN JUEGO

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.

PROFUNDIDAD



ÁREA

app-movil

DOMINIO

Móvil

Hallazgo 6 de 10

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

QUÉ ESTÁ EN JUEGO

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.

ÁREA

settlement-contract

DOMINIO

Smart contract

03 · SEVERIDAD MENOR

Bajas e informativas

BAJA CVSS 3.7 Hallazgo 7 de 10 api-graphql · Web

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

QUÉ ESTÁ EN JUEGO

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.

BAJA CVSS 3.1 Hallazgo 8 de 10 api-graphql · Web

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

QUÉ ESTÁ EN JUEGO

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.

INFO CVSS 0.0 Hallazgo 9 de 10 api-legacy · Servidor

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

QUÉ ESTÁ EN JUEGO

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.

INFO

CVSS 0.0 Hallazgo 10 de 10 api-graphql · Web

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

QUÉ ESTÁ EN JUEGO

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.

RESUMEN EJECUTIVO

Preparado para Taruma Pagos.

Este resumen acompaña al informe técnico, que 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.