

CONFIDENCIAL · ANÁLISIS GRATIS

EJEMPLO FICTICIO

EXPEDIENTE · FREE-TARUMA-PAGOS-EXAMPLE

taruma-pagos.example.

Resumen para dirección

MÉTODO	Lectura pasiva de datos públicos, sin pruebas sobre los sistemas
LEÍDO EL	2026-10-28 12:00 UTC
HALLAZGOS	2 altas · 4 medias · 4 bajas · 4 informativas
ORIGEN	Empresa ficticia. Hallazgos basados en análisis reales.



01 · EL RIESGO DE UN VISTAZO

Qué está en juego

14 hallazgos confirmados: 2 altas, 4 medias, 4 bajas, 4 informativas.

PANORAMA DE RIESGO

Hallazgos por dominio y severidad

	CRÍTICA	ALTA	MEDIA	BAJA	INFO	TOTAL
Web	.	.	1	2	2	5
Servidor	.	.	1	.	.	1
Social	.	1	1	.	.	2
Correo	.	.	1	1	1	3
Dominio	.	1	.	1	1	3
TOTAL	0	2	4	4	4	14

HALLAZGO	ÁREA	SEVERIDAD	PUNTAJE
Hay subdominios que apuntan a servicios que ya no existen	subdominios	ALTA	8.2
Hay 3 equipos de empleados infectados con programas que roban contraseñas	personas	ALTA	8.1
Cualquiera puede enviar correos haciéndose pasar por taruma-pagos.example	correo	MEDIA	6.1
El sitio carga librerías con fallas conocidas	sitio	MEDIA	6.1
Hay dominios casi iguales al de la empresa listos para recibir y enviar correo	marca	MEDIA	5.4
Hay servicios abiertos a internet además del sitio	servidores	MEDIA	5.3
Las respuestas del DNS del dominio no están firmadas (DNSSEC)	dominio	BAJA	3.7

HALLAZGO	ÁREA	SEVERIDAD	PUNTAJE
El correo que recibe la empresa puede viajar sin cifrar	correo	BAJA	3.7
El sitio entrega cookies sin las protecciones básicas	sitio	BAJA	3.1
Faltan las cabeceras de seguridad básicas del sitio	sitio	BAJA	3.1
No hay restricción de quién puede emitir certificados para el dominio	dominio	INFO	0.0
Nadie recibe los reportes de quién usa el nombre del dominio	correo	INFO	0.0
El sitio anuncia qué software y versión usa	sitio	INFO	0.0
No hay un contacto publicado para avisar de fallas de seguridad	sitio	INFO	0.0

02 · EN TÉRMINOS DE NEGOCIO

Los hallazgos para la dirección

Hallazgo 1 de 14

Hay subdominios que apuntan a servicios que ya no existen

CVSS 3.1

8.2

ALTA

PROFUNDIDAD

INFO	
BAJA	
MEDIA	
ALTA	
CRÍTICA	

ÁREA

subdominios

DOMINIO

Dominio

QUÉ ESTÁ EN JUEGO

Quien se quede con el subdominio puede publicar ahí lo que quiera con el nombre de la empresa: una página falsa de acceso, código malicioso o correos que pasan los controles por venir de un subdominio real.

Hallazgo 2 de 14

Hay 3 equipos de empleados infectados con programas que roban contraseñas

CVSS 3.1

8.1

ALTA

PROFUNDIDAD

INFO	
BAJA	
MEDIA	
ALTA	
CRÍTICA	

ÁREA

personas

DOMINIO

Social

QUÉ ESTÁ EN JUEGO

Esos programas se llevan todas las contraseñas guardadas en el navegador, incluidas las del correo, el sistema de gestión o el banco de la empresa. Son hoy una de las formas más comunes de entrar a una empresa sin forzar nada.

EXPOSICIÓN ECONÓMICA

Acceso con contraseñas robadas

El costo depende de qué cuentas se usaban en esos equipos: correo, banco, sistemas internos.

EXPOSICIÓN LEGAL Y REGULATORIA

Si con esas cuentas se accede a datos personales de clientes o empleados, puede nacer la obligación de notificar a la autoridad de datos de cada país.

Orientativo: no constituye asesoramiento legal.

Hallazgo 3 de 14

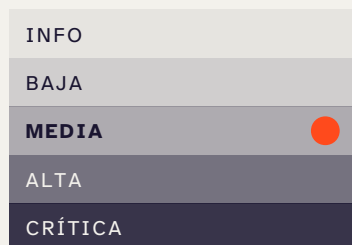
Cualquiera puede enviar correos haciéndose pasar por taruma-pagos.example

CVSS 3.1

6.1

MEDIA

PROFUNDIDAD



ÁREA

correo

DOMINIO

Correo

QUÉ ESTÁ EN JUEGO

Un atacante puede escribirles a sus clientes, proveedores o empleados como si fuera alguien de la empresa: facturas con datos bancarios cambiados, pedidos de pago urgentes o enlaces para robar contraseñas. Las víctimas directas son las personas que confían en sus correos, y el daño a la marca llega aunque la empresa no haya hecho nada. Se cierra con un cambio en el DNS, sin tocar el sitio ni el correo.

EXPOSICIÓN ECONÓMICA

Fraude por correo falso

La pérdida típica es el monto de la factura o el pago desviado, más el costo de recuperar la confianza de quien recibió el correo.

Hallazgo 4 de 14

El sitio carga librerías con fallas conocidas

CVSS 3.1

6.1

MEDIA

PROFUNDIDAD

INFO	
BAJA	
MEDIA	
ALTA	
CRÍTICA	

ÁREA

sitio

DOMINIO

Web

QUÉ ESTÁ EN JUEGO

Varias de estas fallas permiten correr código en el navegador del visitante si el sitio usa la función afectada: robar sesiones, cambiar lo que se muestra o redirigir a una página falsa.

Hallazgo 5 de 14

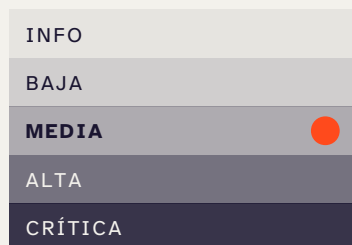
Hay dominios casi iguales al de la empresa listos para recibir y enviar correo

CVSS 3.1

5.4

MEDIA

PROFUNDIDAD



ÁREA

marca

DOMINIO

Social

QUÉ ESTÁ EN JUEGO

Un dominio con una letra cambiada y correo activo es la herramienta clásica del fraude por facturas: el cliente recibe un correo que parece de la empresa, desde una dirección casi idéntica, con datos bancarios nuevos.

EXPOSICIÓN ECONÓMICA

Fraude por correo falso

La pérdida típica es el monto de la factura o el pago desviado.

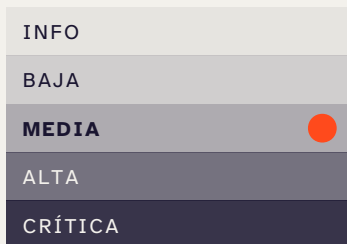
Hallazgo 6 de 14

Hay servicios abiertos a internet además del sitio

CVSS 3.1

5.3**MEDIA**

PROFUNDIDAD



ÁREA

servidores

DOMINIO

Servidor

QUÉ ESTÁ EN JUEGO

Cada servicio abierto (acceso remoto, bases de datos, paneles) es una puerta más que se puede atacar por contraseña o por una falla del software. Muchos ataques automáticos recorren internet buscando justamente estos puertos.

03 · SEVERIDAD MENOR

Bajas e informativas

BAJA CVSS 3.7 Hallazgo 7 de 14 dominio · Dominio

Las respuestas del DNS del dominio no están firmadas (DNSSEC)

QUÉ ESTÁ EN JUEGO

Sin firma, un atacante que logra envenenar un servidor DNS intermedio puede mandar a los visitantes o al correo a un servidor suyo. Es un ataque poco común, y activarlo suele ser una opción del proveedor del dominio.

BAJA CVSS 3.7 Hallazgo 8 de 14 correo · Correo

El correo que recibe la empresa puede viajar sin cifrar

QUÉ ESTÁ EN JUEGO

Alguien con acceso a la red por donde pasa el correo puede forzar que los mensajes viajen sin cifrar y leerlos. Es un ataque difícil, pero el correo de una empresa lleva facturas, contratos y contraseñas.

BAJA CVSS 3.1 Hallazgo 9 de 14 sitio · Web

El sitio entrega cookies sin las protecciones básicas

QUÉ ESTÁ EN JUEGO

Si una de esas cookies identifica la sesión de un usuario, una falla menor en el sitio alcanza para robarla y entrar a su cuenta.

BAJA CVSS 3.1 Hallazgo 10 de 14 sitio · Web

Faltan las cabeceras de seguridad básicas del sitio

QUÉ ESTÁ EN JUEGO

No son una falla por sí solas, pero sin ellas un error en el sitio (un formulario mal validado, un complemento vulnerable) se vuelve mucho más fácil de aprovechar contra los visitantes.

INFO

CVSS 0.0 Hallazgo 11 de 14 dominio · Dominio

No hay restricción de quién puede emitir certificados para el dominio

QUÉ ESTÁ EN JUEGO

Es una capa extra: reduce la chance de que alguien consiga un certificado válido para el dominio engañando a una autoridad poco cuidadosa.

INFO

CVSS 0.0 Hallazgo 12 de 14 correo · Correo

Nadie recibe los reportes de quién usa el nombre del dominio

QUÉ ESTÁ EN JUEGO

Sin esos reportes la empresa no se entera si alguien está enviando correos en su nombre, y no tiene datos para endurecer la política sin cortar envíos propios.

INFO

CVSS 0.0 Hallazgo 13 de 14 sitio · Web

El sitio anuncia qué software y versión usa

QUÉ ESTÁ EN JUEGO

No es una falla, pero les ahorra trabajo a quienes buscan sitios con una versión vulnerable para atacarlos en masa.

INFO

CVSS 0.0 Hallazgo 14 de 14 sitio · Web

No hay un contacto publicado para avisar de fallas de seguridad

QUÉ ESTÁ EN JUEGO

Quien encuentra un problema y no sabe a quién escribir suele publicarlo o abandonarlo. Con un contacto claro, la empresa se entera primero.

04 · PASOS SIGUIENTES

Lo que este análisis no mira

Este análisis lee solo datos públicos de taruma-pagos.example: no entra a tu sitio ni a tus sistemas. Lo que hay adentro lo mira una auditoría, con tu autorización firmada:

US\$4.500

Dig

Tu sitio y tus servidores probados por dentro: el inicio de sesión, los formularios, los pagos y lo que corre detrás.

lop.run/es/servicios/dig

US\$9.500

Rabbit Hole

Tu plataforma entera: las cuentas y los permisos de cada cliente, las API, la lógica del negocio y la nube.

lop.run/es/servicios/rabbit-hole

desde US\$15.000

Warren

Toda tu empresa: además de la plataforma, la red de la oficina, el wifi, el correo y si tu equipo cae en un engaño.

lop.run/es/servicios/warren

US\$490

Sniff

¿No sabes cuál necesitas? Un especialista mira este análisis contigo 30 minutos y te lo dice, con precio cerrado. Si después contratas una auditoría, se descuenta.

lop.run/es/servicios/sniff

Lo que puedes hacer ahora

Gratis

Sello de vigilancia

Revisamos tu dominio una vez por mes, sin pagar, y te escribimos solo si algo cambió.

lop.run/es/servicios/#gratis

US\$449 por mes

Ears + Lop

Vigilamos tu dominio las 24 horas y un especialista confirma cada aviso antes de que te llegue y te dice qué hacer. Este análisis encontró hallazgos graves: con una persona al lado no dependes de interpretar cada alerta.

lop.run/es/servicios/ears-lop

US\$95 la hora (mínimo US\$150)

Lop Fix

Este informe trae 11 arreglos de configuración. Si prefieres no hacerlos tú, los hacemos por ti.

lop.run/es/servicios/lop-fix

RESUMEN PARA DIRECCIÓN

Preparado para taruma- pagos.example.

Este análisis leyó solo datos públicos de taruma-pagos.example el 2026-10-28. Nadie probó ni tocó tus sistemas. Si quieres asesoramiento legal sobre estas obligaciones, podemos ponerte en contacto con abogados especializados.