

CONFIDENCIAL · PAGO

EXEMPLO FICTÍCIO

DOSSIÊ · TARUMA-PAGOS

Taruma Pagos.

Resumo executivo

JANELA	2026-09-01 a 2026-09-30
ESCOPO	6 ativos autorizados
ACHADOS	1 crítica · 1 alta · 4 médias · 2 baixas · 2 informativas
ORIGEM	Empresa fictícia. Achados baseados em auditorias reais.



01 · O RISCO NUM RELANCE

O que está em jogo

10 achados confirmados: 1 crítica, 1 alta, 4 médias, 2 baixas, 2 informativas.

ATENÇÃO IMEDIATA

Confirmamos 1 vulnerabilidade crítica com uma prova que funciona: O login com a Microsoft permite que uma organização externa entre como administrador de uma empresa cliente. O relatório técnico traz a reprodução e a correção. É preciso agir hoje: escreva para security@lop.run.

PANORAMA DE RISCO**Achados por domínio e severidade**

	CRÍTICA	ALTA	MÉDIA	BAIXA	INFO	TOTAL
Web	1	1	1	2	1	6
Smart contract	.	.	1	.	.	1
Servidor	.	.	.	.	1	1
Rede	.	.	1	.	.	1
Mobile	.	.	1	.	.	1
TOTAL	1	1	4	2	2	10

ACHADO	ÁREA	SEVERIDADE	NOTA
O login com a Microsoft permite que uma organização externa entre como administrador de uma empresa cliente	app-web	CRÍTICA	9.1
A página de chaves de API de um cliente fica guardada no cache público e qualquer anônimo pode vê-la	app-web	ALTA	7.4
O limite diário de pagamentos pode ser ultrapassado enviando várias ordens ao mesmo tempo	app-web	MÉDIA	6.5

ACHADO	ÁREA	SEVERIDADE	NOTA
Um subdomínio aponta para um serviço desativado e pode ser tomado por terceiros	dns-taruma	MÉDIA	6.1
O app móvel inclui uma chave de API de um serviço de mapas sem restrição de uso	app-movil	MÉDIA	5.3
Uma ordem assinada no ambiente de testes pode ser executada em produção	settlement-contract	MÉDIA	Impacto alto, probabilidade baixa
Uma biblioteca com uma vulnerabilidade publicada está presente, mas a função afetada não é usada	api-graphql	BAIXA	3.7
O validador de webhooks pode ser apontado para a rede interna, com alcance limitado	api-graphql	BAIXA	3.1
Um host de API legado ainda aceita uma versão obsoleta do TLS	api-legacy	INFO	0.0
A API GraphQL expõe o esquema completo em produção (introspecção ativa)	api-graphql	INFO	0.0

02 · EM TERMOS DE NEGÓCIO

Os achados para a diretoria

Achado 1 de 10

0 login com a Microsoft permite que uma organização externa entre como administrador de uma empresa cliente

CVSS 3.1

9.1**CRÍTICA**

PROFUNDIDADE

INFO

BAIXA

MÉDIA

ALTA

CRÍTICA

ÁREA

app-web

DOMÍNIO

Web

O QUE ESTÁ EM JOGO

Um atacante entra como administrador de qualquer empresa cliente cujo e-mail conheça, sem a senha e sem o segundo fator. A partir daí aprova lotes de pagamento, troca as contas bancárias de destino e vê os dados de todos os fornecedores dessa empresa. É o caminho direto para movimentar fundos e chegar aos dados pessoais, e não deixa rastro de acesso forçado porque o login parece legítimo.

EXPOSIÇÃO FINANCEIRA

USD 250 mil a 3 milhões

Soma os fundos desviados de lotes aprovados em nome de uma empresa cliente, o vazamento dos dados bancários dos seus fornecedores, o custo de resposta e o atraso da rodada de investimento. O limite inferior supõe detecção antes da liquidação; o superior, fundos já liquidados.

EXPOSIÇÃO LEGAL E REGULATÓRIA

Lei 25.326 (Argentina), art. 9, dever de segurança

Lei 19.670 art. 38 e Decreto 64/020 (Uruguai), aviso em 72 horas

LGPD e Res. CD/ANPD 15/2024 (Brasil), comunicação em 3 dias úteis

O acesso a dados bancários e de identidade de fornecedores é um incidente com dados pessoais. Uruguai: comunicar a URCDP em 72 horas. Brasil: comunicar a ANPD e os titulares afetados em 3 dias úteis se houver risco relevante. Argentina: compromete o dever de segurança; comunicar a AAIP é recomendado.

Orientativo: não constitui assessoria jurídica.

Achado 2 de 10

A página de chaves de API de um cliente fica guardada no cache público e qualquer anônimo pode vê-la

CVSS 3.1

7.4**ALTA**

PROFUNDIDADE

INFO

BAIXA

MÉDIA

ALTA

CRÍTICA

ÁREA

app-web

DOMÍNIO

Web

O QUE ESTÁ EM JOGO

Um atacante que consegue fazer a vítima abrir um link preparado deixa a página privada dessa vítima guardada no cache público e depois a recupera sem estar autenticado. Expõe as chaves de API da empresa cliente, que permitem operar na plataforma em nome dela.

EXPOSIÇÃO FINANCEIRA

USD 30 mil a 200 mil

A exposição são as chaves de API das empresas clientes cujos administradores abrirem o link, e o que puder ser operado com elas até a rotação. Cresce com a quantidade de vítimas alcançadas; não é um vazamento em massa de uma só vez.

EXPOSIÇÃO LEGAL E REGULATÓRIA

Lei 25.326 (Argentina), art. 9, dever de segurança

Lei 19.670 art. 38 e Decreto 64/020 (Uruguai), aviso em 72 horas

LGPD e Res. CD/ANPD 15/2024 (Brasil), comunicação em 3 dias úteis

A exposição de credenciais e de dados da conta de um cliente compromete o dever de segurança sobre dados pessoais. Se for confirmado acesso efetivo a dados de pessoas, no Uruguai é preciso comunicar a URCDP em 72 horas e no Brasil a ANPD em 3 dias úteis se houver risco relevante; na Argentina, a AAIP recomenda comunicar.

Orientativo: não constitui assessoria jurídica.

Achado 3 de 10

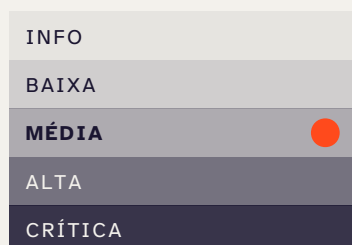
0 limite diário de pagamentos pode ser ultrapassado enviando várias ordens ao mesmo tempo

CVSS 3.1

6.5

MÉDIA

PROFUNDIDADE



ÁREA

app-web

DOMÍNIO

Web

O QUE ESTÁ EM JOGO

Um usuário com permissão para iniciar pagamentos, mas sujeito a um teto diário, consegue ordenar pagamentos muito acima desse teto em um mesmo instante. O teto existe justamente para conter o erro e a fraude interna; sem ele, uma conta comprometida ou um funcionário desonesto movimentaria valores bem acima do previsto antes que alguém perceba.

EXPOSIÇÃO FINANCEIRA

USD 80 mil a 600 mil

A perda é o excesso movimentado acima do teto antes da detecção, limitado pelo saldo disponível da conta e pela janela até a liquidação. A faixa considera tetos diários típicos e a quantidade de ordens que cabem em uma única rajada.

Achado 4 de 10

Um subdomínio aponta para um serviço desativado e pode ser tomado por terceiros

CVSS 3.1

6.1

MÉDIA

PROFUNDIDADE

INFO	
BAIXA	
MÉDIA	●
ALTA	
CRÍTICA	

ÁREA

dns-taruma

DOMÍNIO

Rede

O QUE ESTÁ EM JOGO

Quem tomar o subdomínio pode publicar páginas que parecem oficiais da Tarumá, úteis para enganar clientes ou funcionários e para campanhas de phishing com um domínio legítimo. Prejudica a confiança na marca e facilita o roubo de credenciais.

EXPOSIÇÃO FINANCEIRA

USD 10 mil a 90 mil

O custo é de reputação e de resposta a um uso do subdomínio para enganar clientes; não há perda direta de fundos. A faixa reflete o alcance de uma campanha de phishing com um domínio legítimo.

Achado 5 de 10

0 app móvel inclui uma chave de API de um serviço de mapas sem restrição de uso

CVSS 3.1

5.3

MÉDIA

PROFUNDIDADE

INFO	
BAIXA	
MÉDIA	●
ALTA	
CRÍTICA	

ÁREA

app-movil

DOMÍNIO

Mobile

O QUE ESTÁ EM JOGO

O risco é o consumo da cota do serviço de mapas por conta da Tarumá, com um custo financeiro limitado. Não dá acesso a dados de clientes nem a fundos. Verificamos o alcance da chave sem usá-la para gerar cobranças.

Achado 6 de 10

Uma ordem assinada no ambiente de testes pode ser executada em produção

IMPACTO x PROBABILIDADE

MÉDIA

IMPACTO

Alto

PROBABILIDADE

Baixa

PROFUNDIDADE

INFO

BAIXA

MÉDIA

ALTA

CRÍTICA

O QUE ESTÁ EM JOGO

Uma ordem pensada para o ambiente de testes, onde valores e contrapartes não são reais, pode ser reutilizada para ordenar uma liquidação real em produção. Quebra a separação entre testar e operar, uma das garantias que um banco parceiro e um auditor esperam encontrar.

EXPOSIÇÃO FINANCEIRA

USD 50 mil a 400 mil

O risco é a execução em produção de ordens que nunca foram pensadas como reais. A faixa considera o tamanho típico de uma ordem de liquidação e a quantidade de assinaturas de teste em circulação; não há perda de capital custodiado fora dessas ordens.

ÁREA

settlement-contract

DOMÍNIO

Smart contract

03 · SEVERIDADE MENOR

Baixas e informativas

BAIXA CVSS 3.7 Achado 7 de 10 api-graphql · Web

Uma biblioteca com uma vulnerabilidade publicada está presente, mas a função afetada não é usada

O QUE ESTÁ EM JOGO

Hoje não há um caminho de exploração, então o risco imediato é baixo. Importa mesmo assim porque uma mudança futura no código pode começar a usar a função afetada, e porque convém não carregar dependências com vulnerabilidades conhecidas.

BAIXA CVSS 3.1 Achado 8 de 10 api-graphql · Web

O validador de webhooks pode ser apontado para a rede interna, com alcance limitado

O QUE ESTÁ EM JOGO

Um atacante autenticado consegue fazer a plataforma consultar serviços da rede interna que não deveriam ser alcançáveis de fora. Nesta instalação o impacto está contido porque as credenciais da nuvem estão protegidas; ainda assim é um ponto de apoio para dentro que, combinado com outra fraqueza interna, poderia crescer. É informado como baixo, e não crítico, justamente porque o roubo de credenciais foi bloqueado.

EXPOSIÇÃO FINANCEIRA

USD 15 mil a 120 mil

O impacto direto é o acesso a serviços internos de baixo valor; a faixa reflete um risco de apoio, não um vazamento confirmado, já que o caminho até as credenciais está fechado. O limite superior supõe encadear com outra fraqueza interna.

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

Um host de API legado ainda aceita uma versão obsoleta do TLS

O QUE ESTÁ EM JOGO

Manter uma versão obsoleta da criptografia é um item típico dos questionários de conformidade e dos pedidos de um banco parceiro. O risco prático é baixo enquanto não circular informação sensível por esse host, mas convém fechar antes de uma auditoria formal.

INFO

CVSS 0.0 Achado 10 de 10 api-graphql · Web

A API GraphQL expõe o esquema completo em produção (introspecção ativa)

O QUE ESTÁ EM JOGO

Reduz o esforço de reconhecimento de um atacante: em vez de adivinhar, ele lê o mapa da API. É uma informação útil para quem procura fraquezas, sem ser por si só uma porta de entrada.

RESUMO EXECUTIVO

Preparado para Taruma Pagos.

Este resumo acompanha o relatório técnico, que traz a reprodução e a correção de cada achado confirmado, mais um reteste dentro da janela do trabalho. Se quiser assessoria jurídica sobre essas obrigações, podemos colocar você em contato com advogados especializados.