

CONFIDENCIAL · PAGO

EXEMPLO FICTÍCIO

DOSSIÊ · TARUMA-PAGOS

Taruma Pagos.

Relatório técnico

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.

LOP.run



01 · RESUMO DE RISCO

Achados confirmados

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

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

ID	ATIVO	DOMÍNIO	SEVERIDADE	NOTA	STATUS
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	MÉDIA	6.5	Confirmado
net-subdomain-06	dns-taruma	Rede	MÉDIA	6.1	Confirmado
mob-key-08	app-movil	Mobile	MÉDIA	5.3	Confirmado
sc-sig-03	settlement-contract	Smart contract	MÉDIA	Impacto alto, probabilidade baixa	Confirmado
web-dep-07	api-graphql	Web	BAIXA	3.7	Confirmado

ID	ATIVO	DOMÍNIO	SEVERIDADE	NOTA	STATUS
web-ssrf-05	api-graphql	Web	BAIXA	3.1	Confirmado
net-tls-10	api-legacy	Servidor	INFO	0.0	Confirmado
web-graphql-09	api-graphql	Web	INFO	0.0	Confirmado

02 · DETALHE TÉCNICO

Achados completos

web-sso-01

O 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

ID

web-sso-01

VETOR

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

ATIVO

app-web

DOMÍNIO

Web

STATUS

Confirmado

DESCRIÇÃO

O login federado com a Microsoft identifica o usuário pelo endereço de e-mail que vem no token, e não pelo identificador estável da conta e da sua organização de origem. Como o endereço de e-mail é controlado por quem administra a organização de origem, uma organização externa pode apresentar um token legítimo com o e-mail de um administrador da Tarumá, e a aplicação o aceita como esse administrador. O vínculo entre a conta externa e a conta interna depende de um dado que o atacante escolhe, não de um dado que a Tarumá controla.

IMPACTO NO NEGÓCIO

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.

EVIDÊNCIA

`poc/ingreso.md`

`sha256:79b84512190de5cf4208613eb8d3189c805469fba5796c0c
c5a19527a5c69f93`

Entrada como administrador de teste a partir de uma identidade externa; o controle com a conta verificada é rejeitado

PROVA DE CONCEITO

Demonstramos o acesso como um administrador de teste da Tarumá a partir de uma organização de identidade que nós controlávamos, sem usar nenhuma credencial da vítima. Como controle, o mesmo fluxo com o identificador estável e a organização de origem verificados rejeita a entrada, o que isola a falha: confiar no e-mail, e não na verificação da conta.

CORREÇÃO

Vincular a conta pelo identificador estável do usuário e pelo identificador da sua organização de origem, e não pelo e-mail, e rejeitar a entrada de organizações que não estejam em uma lista autorizada. Não usar o e-mail nem o nome de usuário como identificador: na Microsoft esses dados não provam que a organização de origem é dona do domínio. Para os clientes já cadastrados, vincular de novo as contas ao identificador estável no próximo login.

REVISÃO ADVERSARIAL

Veredito **confirmado** frente a web-bounty OWASP (A07 falhas de identificação e autenticação; confiança no e-mail do token).

- acesso próprio (descartado: a entrada usou uma identidade externa, não a da vítima)
- e-mail verificado que coincide por acaso (descartado: o e-mail foi escolhido pelo atacante)

web-cache-04

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

ID

web-cache-04

VETOR

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

ATIVO

app-web

DOMÍNIO

Web

STATUS

Confirmado

DESCRIÇÃO

A rede de distribuição de conteúdo decide o que guardar no seu cache público olhando a extensão no final do endereço, antes que a aplicação decida se aquela página é privada. Ao pedir a página privada de chaves de API com uma extensão de arquivo estático acrescentada no final, a resposta, que contém dados da sessão da vítima, fica guardada no cache e depois é servida a qualquer pessoa que peça o mesmo endereço. É o padrão conhecido como engano de cache web.

IMPACTO NO NEGÓCIO

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.

EVIDÊNCIA

`poc/cache.md`

```
sha256:1fc65b727a7bbf85e34fe5e123bcfedf232fe54ddff46b4876707334634fb2c1
```

A resposta privada fica no cache e é recuperada sem sessão; o endereço normal não é guardado em cache

PROVA DE CONCEITO

Demonstramos, em uma conta de teste nossa, que a resposta privada é armazenada no cache e recuperada depois sem sessão. O controle com o endereço normal, sem a extensão acrescentada, não é armazenado. Nenhuma conta real de cliente foi usada.

CORREÇÃO

Fazer a decisão de guardar em cache depender dos cabeçalhos que a aplicação envia, e não da extensão do endereço, e marcar toda resposta autenticada como não armazenável. Na rede de distribuição, não guardar por extensão caminhos que podem ser dinâmicos. Rotacionar as chaves de API que possam ter ficado expostas.

REVISÃO ADVERSARIAL

Veredito **confirmado** frente a web-bounty (engano de cache web; interação entre a CDN e a autorização da aplicação).

- conteúdo público (descartado: a página afetada exige sessão e mostra dados do titular)
- cache local do navegador (descartado: a resposta foi recuperada de outra rede sem sessão)

web-race-02

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

CVSS 3.1

6.5

MÉDIA

PROFUNDIDADE

INFO	
BAIXA	
MÉDIA	
ALTA	
CRÍTICA	

ID

web-race-02

VETOR

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

ATIVO

app-web

DOMÍNIO

Web

STATUS

Confirmado

DESCRIÇÃO

O controle do limite diário de pagamentos lê o total acumulado, decide e só depois o atualiza, sem tratar essas etapas como uma única operação indivisível. Quando várias ordens chegam juntas, todas leem o mesmo total anterior e todas passam pelo controle antes que alguma o atualize, e o limite é ultrapassado. É uma condição de corrida clássica no caminho de aprovação de pagamentos.

IMPACTO NO NEGÓCIO

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.

EVIDÊNCIA

poc/limite.md

sha256:225fe2b5c79867ed4f2cb8b513d3ce474f69356d0b4250f1b72afc87d4e661bc

Várias ordens simultâneas cujo total excede o teto são aprovadas; o envio sequencial respeita o teto

PROVA DE CONCEITO

Demonstramos que um conjunto de ordens enviadas ao mesmo tempo, cujo total ultrapassa o teto diário, é aprovado por inteiro, enquanto enviadas uma após a outra a segunda é rejeitada. O controle sequencial confirma que o problema é a simultaneidade, e não o cálculo do teto.

CORREÇÃO

Aplicar o limite dentro de uma transação que bloqueie o registro do acumulado (ou um bloqueio por conta), para que as ordens concorrentes sejam avaliadas em série. Acrescentar uma verificação final antes da liquidação e um teste que dispare várias ordens ao mesmo tempo e espere que só passem as que cabem no teto.

REVISÃO ADVERSARIAL

Veredito **confirmado** frente a web-bounty OWASP (condição de corrida em limites; TOCTOU na aprovação de pagamentos).

- envio duplicado acidental (descartado: cada ordem era distinta e válida)
- teto mal configurado (descartado: o envio sequencial respeita o teto corretamente)

net-subdomain-06

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	

ID

net-subdomain-06

VETOR

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

ATIVO

dns-taruma

DOMÍNIO

Rede

STATUS

Confirmado

DESCRIÇÃO

O subdomínio da página de status do serviço continua apontando, via DNS, para uma plataforma externa onde o recurso já foi desativado. Enquanto esse registro continuar publicado, um terceiro pode criar o recurso nessa plataforma e ficar com o subdomínio, servindo conteúdo com o nome da Tarumá.

IMPACTO NO NEGÓCIO

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.

EVIDÊNCIA

poc/subdominio.md

```
sha256:6899e3ebc8c130e54d55fb5cda8df8a7533e766736b18686019610eace5ae371
```

O subdomínio resolve para uma plataforma externa onde o recurso foi desativado e pode ser tomado

PROVA DE CONCEITO

Verificamos que o subdomínio resolve para uma plataforma externa onde o recurso não existe e que a plataforma permite tomá-lo. Pelas regras do trabalho, ele NÃO foi tomado: apenas confirmamos a condição e guardamos a evidência.

CORREÇÃO

Apagar o registro DNS que ficou órfão, ou retomar o recurso na plataforma externa. Revisar os demais subdomínios em busca de registros que apontem para serviços desativados e incluir essa revisão no monitoramento contínuo.

REVISÃO ADVERSARIAL

Veredito **confirmado** frente a OSINT / superfície (subdomínio que pode ser tomado; verificado sem tomá-lo, pelas regras do trabalho).

- serviço ativo (descartado: o recurso não existe na plataforma de destino)
- subdomínio sem uso (descartado: resolve publicamente e é alcançável)

mob-key-08

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	

ID

mob-key-08

VETOR

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

ATIVO

app-movil

DOMÍNIO

Mobile

STATUS

Confirmado

DESCRIÇÃO

O pacote público do app móvel contém uma chave de API de um serviço de mapas. Qualquer pessoa que inspecione o pacote a obtém. A chave não tem restrição por aplicativo nem por domínio, então pode ser usada fora do app, o que consome a cota paga da Tarumá.

IMPACTO NO NEGÓCIO

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.

EVIDÊNCIA

poc/clave_movil.md

```
sha256:208eb939639cc2556449f0893313ca649901b6c3f223250601e4e4ebcd30e7a5
```

A chave está no pacote público e o serviço a aceita fora do app

PROVA DE CONCEITO

Identificamos a chave no pacote público e confirmamos, com uma consulta de teste sem custo feita fora do app, que o serviço a aceita sem restrição de origem. Não foram feitas consultas que gerassem cobranças.

CORREÇÃO

Restringir a chave por aplicativo e aos serviços que ela realmente usa; rotacioná-la; manter as chaves de terceiros fora do pacote quando o serviço permitir. Revisar o resto do pacote em busca de outros segredos.

REVISÃO ADVERSARIAL

Veredito **confirmado** frente a varredura de segredos do pacote móvel (alcance verificado sem gerar cobranças).

- chave de exemplo (descartado: é a chave de produção do serviço de mapas)
- chave já restrita (descartado: o serviço a aceita fora do app)

sc-sig-03

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

ID

sc-sig-03

ATIVO

settlement-contract

DOMÍNIO

Smart contract

STATUS

Confirmado

DESCRIÇÃO

As ordens de liquidação são autorizadas com uma assinatura sobre dados estruturados. O domínio dessa assinatura não inclui o endereço do contrato que vai executá-la, e os contratos de teste e de produção compartilham o mesmo signatário na mesma rede. Por isso, uma assinatura emitida para uma ordem de teste também vale para o contrato de produção: ela não fica atrelada ao contrato para o qual foi criada.

IMPACTO NO NEGÓCIO

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.

EVIDÊNCIA

poc/firma.md

```
sha256:2b419a151e0a1b674e3012cf584e183318b304441ef4918d867c33a7cd5a5abc
```

Uma ordem assinada para o contrato de testes é aceita pelo de produção; com o domínio atrelado ao contrato, é rejeitada

PROVA DE CONCEITO

Verificamos, com a revisão do código do contrato no commit fixado e um teste em uma cópia da rede, que uma ordem assinada para o contrato de testes é aceita pelo de produção. O controle com o domínio de assinatura atrelado ao endereço do contrato faz a mesma assinatura ser rejeitada.

CORREÇÃO

Incluir o endereço do contrato e o identificador da rede no domínio da assinatura, para que cada assinatura valha apenas para o contrato e a rede para os quais foi criada. Usar signatários diferentes para testes e produção. Verificar se há ordens assinadas anteriores que devam ser invalidadas.

REVISÃO ADVERSARIAL

Veredito **confirmado** frente a sc-bounty (reutilização de assinatura por domínio incompleto; separação de ambientes).

- assinatura reutilizável por design (descartado: nenhum caso de uso exige isso)
- mesmo contrato nos dois ambientes (descartado: são implantações distintas com a mesma chave)

03 · SEVERIDADE MENOR

Baixas e informativas

BAIXA

CVSS 3.7 web-dep-07 api-graphql · Web

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

DESCRIÇÃO

A análise automática de dependências marcou como alta uma biblioteca com uma vulnerabilidade publicada. A análise de alcançabilidade mostra que a função vulnerável não é chamada pelo código da Tarumá por nenhum caminho: a rota necessária para explorá-la não existe nesta aplicação. Por isso é informada como baixa, e não como alta: o risco real é de manutenção, não uma via de ataque ativa hoje.

IMPACTO NO NEGÓCIO

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.

EVIDÊNCIA

poc/dependencia.md

sha256:7fdb1e901c6bc2c4a18944e964db48f711efdb7e5e6dd4930d1194ab07709359

A função vulnerável não é alcançável a partir do código no commit fixado

PROVA DE CONCEITO

Revisamos, no código do commit fixado, que a função vulnerável não é chamada por nenhum caminho alcançável. Registramos a versão instalada e a rota ausente.

CORREÇÃO

Atualizar a biblioteca para uma versão corrigida no próximo ciclo de manutenção. Manter a análise de alcançabilidade no processo, para não tratar todo alerta do scanner como crítico nem descartá-lo sem revisão.

REVISÃO ADVERSARIAL

Veredito **confirmado** frente a SCA e análise de alcançabilidade (severidade ajustada de alta para baixa pelo impacto real).

- falso positivo do scanner (descartado: a biblioteca e a versão existem)
- função vulnerável em uso (descartado pela análise de alcançabilidade)

BAIXA

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

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

DESCRIÇÃO

Ao cadastrar um webhook, a plataforma consulta o endereço informado para validá-lo. Um nome de domínio sob controle do atacante pode resolver primeiro para um endereço externo (para passar na validação) e depois para um endereço interno (quando a plataforma faz a consulta real), técnica conhecida como DNS rebinding. Assim a consulta sai para a rede interna. Importante: o serviço de metadados da nuvem exige o método reforçado (IMDSv2), que está ativo, por isso NÃO foi possível obter credenciais da nuvem; o alcance se limita a confirmar que serviços internos são alcançáveis.

IMPACTO NO NEGÓCIO

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.

EVIDÊNCIA

`poc/webhook.md`

`sha256:6994745f10858afc08cd7f269a7e501e653da04cbcf8c1f32c5491656641644c`

A consulta de validação alcança um serviço interno; o acesso ao serviço de metadados é rejeitado

PROVA DE CONCEITO

Confirmamos que um endereço sob nosso controle, redirecionado para um endereço interno, faz a plataforma consultá-lo, e que a tentativa de alcançar o serviço de metadados da nuvem é rejeitada pelo método reforçado. O controle com um endereço que sempre resolve para um externo se comporta como esperado.

CORREÇÃO

Resolver o nome uma única vez e validar o mesmo endereço que depois é consultado (para que não mude entre a validação e o uso); rejeitar endereços de faixas internas e de link local; fazer as consultas de webhook a partir de uma rede sem acesso a serviços internos. Manter o IMDSv2 obrigatório.

REVISÃO ADVERSARIAL

Veredito **confirmado** frente a web-bounty (SSRF por DNS rebinding; impacto verificado contra o serviço de metadados).

- destino legítimo mal classificado (descartado: o endereço final era de uma faixa interna)
- acesso a credenciais da nuvem (descartado e verificado: o IMDSv2 bloqueia)

INFO

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

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

DESCRIÇÃO

O host da API legada aceita TLS 1.0, uma versão do protocolo de criptografia considerada obsoleta e retirada dos requisitos do setor. Não foi observado tráfego sensível ativo nesse host, então o risco real é de conformidade e de higiene, não uma exposição direta hoje.

IMPACTO NO NEGÓCIO

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.

EVIDÊNCIA

poc/tls.md

sha256:1ba53d90348571db8172e0ef2d81c53b9a41d61788c6c3b0bf94671ae2f8ac26

O host negocia TLS 1.0 além das versões atuais

PROVA DE CONCEITO

Verificamos com um teste da configuração de criptografia que o host negocia TLS 1.0, além das versões atuais.

CORREÇÃO

Desabilitar TLS 1.0 e 1.1 e deixar apenas TLS 1.2 e 1.3 no host legado. Incluir a postura de criptografia no monitoramento contínuo para detectar regressões.

REVISÃO ADVERSARIAL

Veredito **confirmado** frente a infraestrutura / TLS (versão obsoleta do protocolo em um host legado).

- host sem uso (descartado: responde e negocia a conexão)

INFO

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

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

DESCRIÇÃO

A consulta de introspecção está habilitada em produção, então qualquer pessoa obtém o esquema completo da API: todos os tipos, campos e operações, inclusive os que a aplicação não usa. Não é uma falha por si só, mas entrega a um atacante o mapa da API e facilita encontrar operações pouco protegidas.

IMPACTO NO NEGÓCIO

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.

EVIDÊNCIA

`poc/introspeccion.md`

`sha256:1bdbb5c262c6328a01a84d6a31d975599aa8d342ef8cb452091b0740782ed30f`

A consulta de introspecção devolve o esquema completo em produção

PROVA DE CONCEITO

Obtivemos o esquema completo com uma consulta de introspecção contra o ambiente de produção.

CORREÇÃO

Desabilitar a introspecção em produção e mantê-la apenas nos ambientes de desenvolvimento. Verificar se as operações sensíveis têm a sua própria autorização, sem depender de o esquema ser pouco conhecido.

REVISÃO ADVERSARIAL

Veredito **confirmado** frente a superfície de ataque (introspecção de GraphQL em produção).

- ambiente de desenvolvimento (descartado: a consulta foi contra produção)

RELATÓRIO TÉCNICO

Preparado para Taruma Pagos.

Este relatório 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.