

CONFIDENTIAL · PAID

FICTIONAL SAMPLE

CASE FILE · TARUMA-PAGOS

Taruma Pagos.

Executive summary

WINDOW	2026-09-01 to 2026-09-30
SCOPE	6 authorized assets
FINDINGS	1 critical · 1 high · 4 medium · 2 low · 2 informational
BASIS	Fictional company. Findings based on real audits.

LOP.run



01 · RISK AT A GLANCE

What is at stake

10 confirmed findings: 1 critical, 1 high, 4 medium, 2 low, 2 informational.

IMMEDIATE ATTENTION

We confirmed 1 critical vulnerability with a working proof: Sign-in with Microsoft lets an outside organization log in as the administrator of a client company. The technical report has the reproduction and the fix. It calls for action today: write to security@lop.run.

RISK OVERVIEW**Findings by domain and severity**

	CRITICAL	HIGH	MEDIUM	LOW	INFO	TOTAL
Web	1	1	1	2	1	6
Smart contract	.	.	1	.	.	1
Server	.	.	.	.	1	1
Network	.	.	1	.	.	1
Mobile	.	.	1	.	.	1
TOTAL	1	1	4	2	2	10

FINDING	AREA	SEVERITY	SCORE
Sign-in with Microsoft lets an outside organization log in as the administrator of a client company	app-web	CRITICAL	9.1
A client's API key page is stored in the public cache and an anonymous visitor can see it	app-web	HIGH	7.4
The daily payment limit can be exceeded by sending several orders at the same time	app-web	MEDIUM	6.5
A subdomain points to a decommissioned service and can be claimed by a third party	dns-taruma	MEDIUM	6.1

FINDING	AREA	SEVERITY	SCORE
The mobile app ships a map service API key with no usage restriction	app-movil	MEDIUM	5.3
An order signed in the test environment can be executed in production	settlement-contract	MEDIUM	Impact high, likelihood low
A library with a published vulnerability is present, but the affected function is not used	api-graphql	LOW	3.7
The webhook validator can be pointed at the internal network, with limited reach	api-graphql	LOW	3.1
A legacy API host still accepts an obsolete TLS version	api-legacy	INFO	0.0
The GraphQL API exposes its full schema in production (introspection enabled)	api-graphql	INFO	0.0

02 · IN BUSINESS TERMS

The findings for management

Finding 1 of 10

Sign-in with Microsoft lets an outside organization log in as the administrator of a client company

CVSS 3.1

9.1**CRITICAL**

DEPTH

INFO

LOW

MEDIUM

HIGH

CRITICAL

AREA

app-web

DOMAIN

Web

WHAT IS AT STAKE

An attacker logs in as the administrator of any client company whose email they know, with no password and no second factor. From there they approve payment batches, change the destination bank accounts and see the data of every supplier of that company. It is the direct path to moving funds and to personal data, and it leaves no trace of a forced entry because the sign-in looks legitimate.

FINANCIAL EXPOSURE

USD 250k to 3M

Adds up the funds diverted from batches approved on behalf of a client company, the leak of its suppliers' bank data, the cost of the response and the delay of the funding round. The low end assumes detection before settlement; the high end, funds already settled.

LEGAL AND REGULATORY EXPOSURE

Law 25,326 (Argentina), art. 9, duty of security

Law 19,670 art. 38 and Decree 64/020 (Uruguay), notice within 72 hours

LGPD and ANPD Res. 15/2024 (Brazil), notice within 3 business days

Access to the bank and identity data of suppliers is an incident involving personal data. Uruguay: notify the URCDP within 72 hours. Brazil: notify the ANPD and the people affected within 3 business days if there is relevant risk. Argentina: it compromises the duty of security; notifying the AAIP is recommended.

Indicative only: this is not legal advice.

Finding 2 of 10

A client's API key page is stored in the public cache and an anonymous visitor can see it

CVSS 3.1

7.4**HIGH**

DEPTH

INFO	
LOW	
MEDIUM	
HIGH	
CRITICAL	

AREA

app-web

DOMAIN

Web

WHAT IS AT STAKE

An attacker who gets the victim to open a crafted link leaves that victim's private page in the public cache, and then retrieves it without signing in. It exposes the client company's API keys, which allow operating on the platform in its name.

FINANCIAL EXPOSURE

USD 30k to 200k

The exposure is the API keys of the client companies whose administrators open the link, and whatever can be operated with them until they are rotated. It scales with the number of victims reached; it is not a mass leak in a single step.

LEGAL AND REGULATORY EXPOSURE

Law 25,326 (Argentina), art. 9, duty of security

Law 19,670 art. 38 and Decree 64/020 (Uruguay), notice within 72 hours

LGPD and ANPD Res. 15/2024 (Brazil), notice within 3 business days

Exposing a client's credentials and account data compromises the duty of security over personal data. If effective access to personal data is confirmed, Uruguay requires notifying the URCDP within 72 hours and Brazil the ANPD within 3 business days when there is relevant risk; in Argentina, the AAIP recommends notifying.

Indicative only: this is not legal advice.

Finding 3 of 10

The daily payment limit can be exceeded by sending several orders at the same time

CVSS 3.1

6.5**MEDIUM**

DEPTH

INFO	
LOW	
MEDIUM	
HIGH	
CRITICAL	

AREA

app-web

DOMAIN

Web

WHAT IS AT STAKE

A user allowed to start payments, but held to a daily cap, can order payments for far more than that cap at a single moment. The cap exists precisely to contain mistakes and insider fraud; without it, a compromised account or a dishonest employee moves amounts well above plan before anyone notices.

FINANCIAL EXPOSURE

USD 80k to 600k

The loss is the excess moved above the cap before detection, bounded by the account's available balance and the window until settlement. The band uses typical daily caps and the number of orders that fit in a single burst.

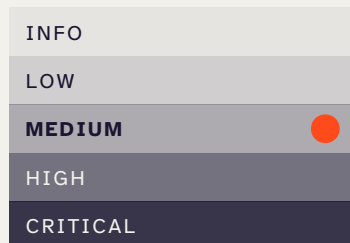
Finding 4 of 10

A subdomain points to a decommissioned service and can be claimed by a third party

CVSS 3.1

6.1**MEDIUM**

DEPTH



AREA

dns-taruma

DOMAIN

Network

WHAT IS AT STAKE

Whoever claims the subdomain can publish pages that look like official Tarumá pages, useful for deceiving clients or employees and for phishing campaigns from a legitimate domain. It damages trust in the brand and makes credential theft easier.

FINANCIAL EXPOSURE**USD 10k to 90k**

The cost is reputational plus the response to the subdomain being used to deceive clients; there is no direct loss of funds. The band reflects the reach of a phishing campaign from a legitimate domain.

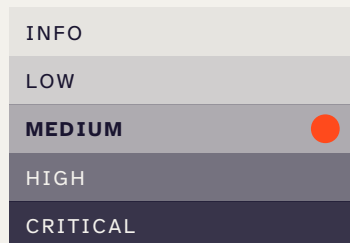
Finding 5 of 10

The mobile app ships a map service API key with no usage restriction

CVSS 3.1

5.3**MEDIUM**

DEPTH



AREA

app-movil

DOMAIN

Mobile

WHAT IS AT STAKE

The risk is consumption of the map service quota at Tarumá's expense, with a bounded financial cost. It gives no access to client data or to funds. We verified the reach of the key without using it to generate charges.

Finding 6 of 10

An order signed in the test environment can be executed in production

IMPACT × LIKELIHOOD

MEDIUM

IMPACT

High

LIKELIHOOD

Low

DEPTH

INFO

LOW

MEDIUM

HIGH

CRITICAL

AREA

settlement-contract

DOMAIN

Smart contract

WHAT IS AT STAKE

An order meant for the test environment, where the amounts and the other parties are not real, can be reused to order a real settlement in production. It breaks the separation between testing and operating, one of the guarantees a partner bank and an auditor expect to find.

FINANCIAL EXPOSURE

USD 50k to 400k

The risk is the execution in production of orders that were never meant to be real. The band uses the typical size of a settlement order and the number of test signatures in circulation; there is no loss of capital held in custody outside those orders.

03 · LOWER SEVERITY

Low and informational

LOW CVSS 3.7 Finding 7 of 10 api-graphql · Web

A library with a published vulnerability is present, but the affected function is not used

WHAT IS AT STAKE

There is no exploitation path today, so the immediate risk is low. It still matters because a future code change could start using the affected function, and because it is wise not to carry dependencies with known vulnerabilities.

LOW CVSS 3.1 Finding 8 of 10 api-graphql · Web

The webhook validator can be pointed at the internal network, with limited reach

WHAT IS AT STAKE

An authenticated attacker can make the platform call internal network services that should not be reachable from outside. In this setup the impact is contained because the cloud credentials are protected; it is still a foothold inward that, combined with another internal weakness, could grow. It is reported as low, not critical, precisely because credential theft was blocked.

FINANCIAL EXPOSURE

USD 15k to 120k

The direct impact is access to low-value internal services; the band reflects a foothold risk, not a confirmed leak, since the path to credentials is closed. The high end assumes chaining with another internal weakness.

INFO CVSS 0.0 Finding 9 of 10 api-legacy · Server

A legacy API host still accepts an obsolete TLS version

WHAT IS AT STAKE

Keeping an obsolete encryption version is a typical item on compliance questionnaires and on the requests of a partner bank. The practical risk is low as long as no sensitive information flows through that host, but it is worth closing before a formal audit.

INFO

CVSS 0.0 Finding 10 of 10 api-graphql · Web

The GraphQL API exposes its full schema in production (introspection enabled)

WHAT IS AT STAKE

It lowers an attacker's reconnaissance effort: instead of guessing, they read the map of the API. It is useful information for anyone looking for weaknesses, without being a way in on its own.

EXECUTIVE SUMMARY

Prepared for Taruma Pagos.

This summary comes with the technical report, which gives the reproduction and the fix for every confirmed finding, plus a retest inside the engagement window. If you want legal advice on these obligations, we can put you in touch with specialized lawyers.