

CONFIDENTIAL · PAID

FICTIONAL SAMPLE

CASE FILE · TARUMA-PAGOS

# Taruma Pagos. Technical report

|          |                                                          |
|----------|----------------------------------------------------------|
| 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 SUMMARY

# Confirmed findings

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

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    |

| ID               | ASSET               | DOMAIN         | SEVERITY | SCORE                       | STATUS    |
|------------------|---------------------|----------------|----------|-----------------------------|-----------|
| web-sso-01       | app-web             | Web            | CRITICAL | 9.1                         | Confirmed |
| web-cache-04     | app-web             | Web            | HIGH     | 7.4                         | Confirmed |
| web-race-02      | app-web             | Web            | MEDIUM   | 6.5                         | Confirmed |
| net-subdomain-06 | dns-taruma          | Network        | MEDIUM   | 6.1                         | Confirmed |
| mob-key-08       | app-movil           | Mobile         | MEDIUM   | 5.3                         | Confirmed |
| sc-sig-03        | settlement-contract | Smart contract | MEDIUM   | Impact high, likelihood low | Confirmed |
| web-dep-07       | api-graphql         | Web            | LOW      | 3.7                         | Confirmed |

| ID             | ASSET       | DOMAIN | SEVERITY | SCORE | STATUS    |
|----------------|-------------|--------|----------|-------|-----------|
| web-ssrf-05    | api-graphql | Web    | LOW      | 3.1   | Confirmed |
| net-tls-10     | api-legacy  | Server | INFO     | 0.0   | Confirmed |
| web-graphql-09 | api-graphql | Web    | INFO     | 0.0   | Confirmed |

## 02 · TECHNICAL DETAIL

# Findings in full

web-sso-01

## 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**

ID

web-sso-01

VECTOR

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

ASSET

app-web

DOMAIN

Web

STATUS

Confirmed

**DESCRIPTION**

Federated sign-in with Microsoft identifies the user by the email address carried in the token, not by the stable account identifier and its home organization. Since the email address is controlled by whoever administers the home organization, an outside organization can present a legitimate token with the email of a Tarumá administrator, and the application accepts it as that administrator. The link between the external account and the internal one rests on a value the attacker chooses, not on one Tarumá controls.

**BUSINESS IMPACT**

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.

## EVIDENCE

`poc/ingreso.md`

```
sha256:79b84512190de5cf4208613eb8d3189c805469fba5796c0c  
c5a19527a5c69f93
```

Sign-in as a test administrator from an external identity; the control with the verified account is rejected

## PROOF OF CONCEPT

We showed access as a Tarumá test administrator from an identity organization we controlled, without using any of the victim's credentials. As a control, the same flow with the stable identifier and the home organization verified rejects the sign-in, which isolates the flaw: trusting the email, not the account check.

## REMEDIATION

Link the account by the user's stable identifier and the identifier of their home organization, not by the email, and reject sign-ins from organizations that are not on an allowed list. Do not use the email or the username as an identifier: in Microsoft those values do not prove that the home organization owns the domain. For clients already signed up, re-link the accounts against the stable identifier at their next session.

## ADVERSARIAL REVIEW

Verdict **confirmed** against web-bounty OWASP (A07 identification and authentication failures; trust in the token email).

- own access (ruled out: the sign-in used an external identity, not the victim's)
- verified email matching by chance (ruled out: the attacker chose the email)

web-cache-04

# 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

ID

web-cache-04

VECTOR

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

ASSET

app-web

DOMAIN

Web

STATUS

Confirmed

## DESCRIPTION

The content delivery network decides what to store in its public cache by looking at the extension at the end of the address, before the application decides whether that page is private. When the private API key page is requested with a static file extension added at the end, the response, which holds the victim's session data, is stored in the cache and then served to anyone who requests that same address. This is the pattern known as web cache deception.

## BUSINESS IMPACT

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.

## EVIDENCE

### poc/cache.md

```
sha256:1fc65b727a7bbf85e34fe5e123bcfedf232fe54ddff46b4876707334634fb2c1
```

The private response stays in the cache and is retrieved without a session; the normal address is not cached

## PROOF OF CONCEPT

We showed, on a test account of our own, that the private response is stored in the cache and later retrieved without a session. The control with the normal address, without the added extension, is not stored. No real client account was used.

## REMEDIATION

Make the caching decision depend on the headers the application sends, not on the address extension, and mark every authenticated response as not cacheable. On the content delivery network, do not cache by extension on paths that can be dynamic. Rotate any API keys that may have been exposed.

## ADVERSARIAL REVIEW

Verdict **confirmed** against web-bounty (web cache deception; interaction between the CDN and the app's authorization).

- public content (ruled out: the affected page requires a session and shows the account holder's data)
- local browser cache (ruled out: the response was retrieved from another network without a session)

web-race-02

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

CVSS 3.1

**6.5****MEDIUM**

DEPTH



ID

web-race-02

VECTOR

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

ASSET

app-web

DOMAIN

Web

STATUS

Confirmed

## DESCRIPTION

The daily payment limit check reads the running total, decides, and only then updates it, without treating those steps as a single indivisible operation. When several orders arrive together, they all read the same previous total and all pass the check before any of them updates it, so the limit is exceeded. It is a classic race condition in the payment approval path.

## BUSINESS IMPACT

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.

## EVIDENCE

**poc/limite.md**

```
sha256:225fe2b5c79867ed4f2cb8b513d3ce474f69356d0b4250f1b72afc87d4e661bc
```

Several simultaneous orders whose total exceeds the cap are approved; sending them one by one respects the cap

## PROOF OF CONCEPT

We showed that a set of orders sent at once, whose total exceeds the daily cap, are all approved, while sent one after another the second is rejected. The one-by-one control confirms that the problem is the concurrency and not the cap calculation.

### REMEDIATION

Enforce the limit inside a transaction that locks the running-total record (or a per-account lock), so concurrent orders are evaluated in sequence. Add a final check before settlement and a test that fires several orders at once and expects only those that fit under the cap to pass.

### ADVERSARIAL REVIEW

Verdict **confirmed** against web-bounty OWASP (race condition on limits; TOCTOU in payment approval).

- accidental double submit (ruled out: each order was distinct and valid)
- wrongly configured cap (ruled out: sequential submission respects the cap correctly)

net-subdomain-06

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

CVSS 3.1

**6.1****MEDIUM**

DEPTH

|               |         |
|---------------|---------|
| INFO          |         |
| LOW           |         |
| <b>MEDIUM</b> | <b></b> |
| HIGH          |         |
| CRITICAL      |         |

ID

net-subdomain-06

VECTOR

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

ASSET

dns-taruma

DOMAIN

Network

STATUS

Confirmed

## DESCRIPTION

The subdomain of the service status page still points, through DNS, to an external platform where the resource was already decommissioned. While that record stays published, a third party can register the resource on that platform and take over the subdomain, serving content under the Tarumá name.

## BUSINESS IMPACT

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.

## EVIDENCE

**poc/subdominio.md**

```
sha256:6899e3ebc8c130e54d55fb5cda8df8a7533e766736b18686019610eace5ae371
```

The subdomain resolves to an external platform where the resource was decommissioned and can be claimed

## PROOF OF CONCEPT

We verified that the subdomain resolves to an external platform where the resource does not exist and that the platform allows claiming it. Under the rules of engagement it was NOT claimed: we only confirmed the condition and kept the evidence.

### REMEDIATION

Delete the dangling DNS record, or take the resource back on the external platform. Check the rest of the subdomains for records pointing to decommissioned services and add that check to continuous monitoring.

### ADVERSARIAL REVIEW

Verdict **confirmed** against OSINT / surface (claimable subdomain; verified without claiming it, under the rules of engagement).

- active service (ruled out: the resource does not exist on the target platform)
- unused subdomain (ruled out: it resolves publicly and is reachable)

mob-key-08

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

CVSS 3.1

**5.3****MEDIUM**

DEPTH

|               |         |
|---------------|---------|
| INFO          |         |
| LOW           |         |
| <b>MEDIUM</b> | <b></b> |
| HIGH          |         |
| CRITICAL      |         |

ID

mob-key-08

VECTOR

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

ASSET

app-movil

DOMAIN

Mobile

STATUS

Confirmed

## DESCRIPTION

The public package of the mobile app contains an API key for a map service. Anyone who inspects the package gets it. The key has no restriction by app or by domain, so it can be used from outside the app, which consumes Tarumá's paid quota.

## BUSINESS IMPACT

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.

## EVIDENCE

**poc/clave\_movil.md**

```
sha256:208eb939639cc2556449f0893313ca649901b6c3f223250601e4e4ebcd30e7a5
```

The key is in the public package and the service accepts it from outside the app

## PROOF OF CONCEPT

We found the key in the public package and confirmed, with a free test query made from outside the app, that the service accepts it with no origin restriction. No queries that would generate charges were made.

#### REMEDIATION

Restrict the key by app and to the services it actually uses; rotate it; keep third-party keys out of the package when the service allows it. Check the rest of the package for other secrets.

#### ADVERSARIAL REVIEW

Verdict **confirmed** against secret scan of the mobile package (reach verified without generating charges).

- sample key (ruled out: it is the production key of the map service)
- key already restricted (ruled out: the service accepts it from outside the app)

sc-sig-03

# 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

### ID

sc-sig-03

### ASSET

settlement-contract

### DOMAIN

Smart contract

### STATUS

Confirmed

## DESCRIPTION

Settlement orders are authorized with a signature over structured data. The domain of that signature does not include the address of the contract that will execute it, and the test and production contracts share the same signer on the same network. As a result, a signature issued for a test order is also valid for the production contract: it is not bound to the contract it was created for.

## BUSINESS IMPACT

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.

## EVIDENCE

**poc/firma.md**

```
sha256:2b419a151e0a1b674e3012cf584e183318b304441ef4918d867c33a7cd5a5abc
```

An order signed for the test contract is accepted by the production one; with the domain bound to the contract it is rejected

## PROOF OF CONCEPT

We verified, by reviewing the contract code at the pinned commit and testing on a copy of the network, that an order signed for the test contract is accepted by the production one. The control with the signing domain bound to the contract address makes the same signature fail.

### REMEDIATION

Include the contract address and the network identifier in the signing domain, so that each signature is valid only for the contract and the network it was created for. Use separate signers for testing and production. Check whether earlier signed orders should be invalidated.

### ADVERSARIAL REVIEW

Verdict **confirmed** against sc-bounty (signature reuse through an incomplete domain; environment separation).

- signature reusable by design (ruled out: no use case requires it)
- same contract in both environments (ruled out: they are separate deployments with the same key)

## 03 · LOWER SEVERITY

# Low and informational

---

LOW

CVSS 3.7 web-dep-07 api-graphql · Web

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

### DESCRIPTION

The automated dependency scan flagged as high a library with a published vulnerability. The reachability analysis shows that the vulnerable function is not called from Tarumá's code along any path: the route needed to exploit it does not exist in this application. That is why it is reported as low, not high: the real risk is maintenance, not an active attack path today.

### BUSINESS IMPACT

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.

### EVIDENCE

poc/dependencia.md

sha256:7fdb1e901c6bc2c4a18944e964db48f711efdb7e5e6dd4930d1194ab07709359

The vulnerable function is not reachable from the code at the pinned commit

### PROOF OF CONCEPT

We checked, on the code at the pinned commit, that the vulnerable function is not called along any reachable path. We recorded the installed version and the missing route.

### REMEDIATION

Upgrade the library to a fixed version in the next maintenance cycle. Keep reachability analysis in the process, so that no scanner alert is treated as critical or dismissed without review.

### ADVERSARIAL REVIEW

Verdict **confirmed** against SCA plus reachability analysis (severity adjusted from high to low by real impact).

- scanner false positive (ruled out: the library and the version exist)
- vulnerable function in use (ruled out by the reachability analysis)

LOW

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

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

### DESCRIPTION

When a webhook is registered, the platform calls the given address to validate it. A domain name under the attacker's control can resolve first to an external address (to pass validation) and then to an internal one (when the platform makes the real call), a technique known as DNS rebinding. That way the call goes out to the internal network. Note: the cloud metadata service requires the hardened method (IMDSv2), which is enabled, so cloud credentials could NOT be obtained; the reach is limited to confirming that internal services can be reached.

### BUSINESS IMPACT

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.

### EVIDENCE

poc/webhook.md

sha256:6994745f10858afc08cd7f269a7e501e653da04cbcf8c1f32c5491656641644c

The validation call reaches an internal service; access to the metadata service is rejected

### PROOF OF CONCEPT

We confirmed that an address under our control, rebound to an internal address, makes the platform call it, and that the attempt to reach the cloud metadata service is rejected by the hardened method. The control with an address that always resolves to an external one behaves as expected.

### REMEDIATION

Resolve the name once and validate that same address, which is then called (so it cannot change between validation and use); reject internal and link-local ranges; make webhook calls from a network with no access to internal services. Keep IMDSv2 mandatory.

### ADVERSARIAL REVIEW

Verdict **confirmed** against web-bounty (SSRF through DNS rebinding; impact checked against the metadata service).

- legitimate destination misclassified (ruled out: the final address was in an internal range)
- access to cloud credentials (ruled out and verified: IMDSv2 blocks it)

## INFO

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

## A legacy API host still accepts an obsolete TLS version

### DESCRIPTION

The legacy API host accepts TLS 1.0, a version of the encryption protocol considered obsolete and dropped from industry requirements. No active sensitive traffic was observed on that host, so the real risk is compliance and hygiene, not a direct exposure today.

### BUSINESS IMPACT

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.

### EVIDENCE

poc/tls.md

sha256:1ba53d90348571db8172e0ef2d81c53b9a41d61788c6c3b0bf94671ae2f8ac26

The host negotiates TLS 1.0 in addition to the current versions

### PROOF OF CONCEPT

We verified with a test of the encryption settings that the host negotiates TLS 1.0, in addition to the current versions.

### REMEDIATION

Disable TLS 1.0 and 1.1 and keep only TLS 1.2 and 1.3 on the legacy host. Add the encryption posture to continuous monitoring to catch regressions.

### ADVERSARIAL REVIEW

Verdict **confirmed** against infrastructure / TLS (obsolete protocol version on a legacy host).

- unused host (ruled out: it responds and negotiates the connection)

## INFO

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

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

### DESCRIPTION

The introspection query is enabled in production, so anyone can get the full schema of the API: every type, field and operation, including those the application does not use. It is not a flaw by itself, but it hands an attacker the map of the API and makes poorly protected operations easier to find.

### BUSINESS IMPACT

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.

## EVIDENCE

`poc/introspeccion.md`

`sha256:1bdbb5c262c6328a01a84d6a31d975599aa8d342ef8cb452091b0740782ed30f`

The introspection query returns the full schema in production

## PROOF OF CONCEPT

We obtained the full schema with an introspection query against the production environment.

## REMEDIATION

Disable introspection in production and keep it only in development environments. Check that sensitive operations have their own authorization, without relying on the schema being little known.

## ADVERSARIAL REVIEW

Verdict **confirmed** against attack surface (GraphQL introspection in production).

- development environment (ruled out: the query ran against production)

TECHNICAL REPORT

# Prepared for Taruma Pagos.

This report 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.