

CONFIDENTIAL · FREE ANALYSIS

FICTIONAL SAMPLE

CASE FILE · FREE-TARUMA-PAGOS-EXAMPLE

taruma-pagos.example. Leadership brief

METHOD	Passive reading of public data, no test on the systems
READ ON	2026-10-28 12:00 UTC
FINDINGS	2 high · 4 medium · 4 low · 4 informational
BASIS	Fictional company. Findings based on real analyses.

LOP.run



01 · RISK AT A GLANCE

What is at stake

14 confirmed findings: 2 high, 4 medium, 4 low, 4 informational.

RISK OVERVIEW

Findings by domain and severity

	CRITICAL	HIGH	MEDIUM	LOW	INFO	TOTAL
Web	.	.	1	2	2	5
Server	.	.	1	.	.	1
Social	.	1	1	.	.	2
Email	.	.	1	1	1	3
Domain	.	1	.	1	1	3
TOTAL	0	2	4	4	4	14

FINDING	AREA	SEVERITY	SCORE
There are subdomains pointing to services that no longer exist	subdomains	HIGH	8.2
3 employee computers are infected with password-stealing programs	people	HIGH	8.1
Anyone can send email in the name of taruma-pagos.example	email	MEDIUM	6.1
The website loads libraries with known flaws	website	MEDIUM	6.1
There are domains almost identical to the company's, ready to send and receive email	brand	MEDIUM	5.4
There are services open to the internet besides the website	servers	MEDIUM	5.3
The domain's DNS answers are not signed (DNSSEC)	domain	LOW	3.7
Email the company receives can travel without encryption	email	LOW	3.7

FINDING	AREA	SEVERITY	SCORE
The website hands out cookies without the basic protections	website	LOW	3.1
The website is missing its basic security headers	website	LOW	3.1
Nothing restricts who can issue certificates for the domain	domain	INFO	0.0
Nobody receives the reports on who uses the domain's name	email	INFO	0.0
The website announces which software and version it runs	website	INFO	0.0
There is no published contact for reporting security flaws	website	INFO	0.0

02 · IN BUSINESS TERMS

The findings for management

Finding 1 of 14

There are subdomains pointing to services that no longer exist

CVSS 3.1

8.2**HIGH**

DEPTH

INFO	
LOW	
MEDIUM	
HIGH	
CRITICAL	

AREA

subdomains

DOMAIN

Domain

WHAT IS AT STAKE

Whoever takes over the subdomain can publish anything there in the company's name: a fake login page, malicious code or emails that pass the checks because they come from a real subdomain.

Finding 2 of 14

3 employee computers are infected with password-stealing programs

CVSS 3.1

8.1**HIGH**

DEPTH



AREA

people

DOMAIN

Social

WHAT IS AT STAKE

Those programs take every password saved in the browser, including the ones for the company's email, management system or bank. They are now one of the most common ways into a company without forcing anything.

FINANCIAL EXPOSURE

Access with stolen passwords

The cost depends on which accounts were used on those computers: email, bank, internal systems.

LEGAL AND REGULATORY EXPOSURE

If those accounts are used to reach personal data of customers or employees, a duty to notify the data protection authority of each country may arise.

Indicative only: this is not legal advice.

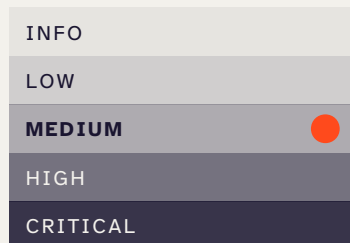
Finding 3 of 14

Anyone can send email in the name of taruma-pagos.example

CVSS 3.1

6.1**MEDIUM**

DEPTH



AREA

email

DOMAIN

Email

WHAT IS AT STAKE

An attacker can write to your customers, suppliers or employees as if they were someone at the company: invoices with changed bank details, urgent payment requests or links that steal passwords. The direct victims are the people who trust your emails, and the damage to the brand comes even though the company did nothing. It is closed with one DNS change, without touching the website or the mailbox.

FINANCIAL EXPOSURE

Fake email fraud

The typical loss is the amount of the diverted invoice or payment, plus the cost of winning back the trust of whoever received the email.

Finding 4 of 14

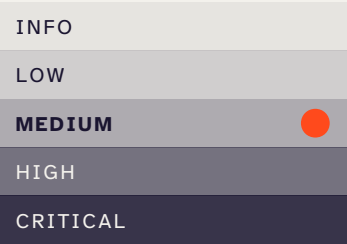
The website loads libraries with known flaws

CVSS 3.1

6.1

MEDIUM

DEPTH



AREA

website

DOMAIN

Web

WHAT IS AT STAKE

Several of these flaws let code run in the visitor's browser if the website uses the affected function: stealing sessions, changing what is shown or redirecting to a fake page.

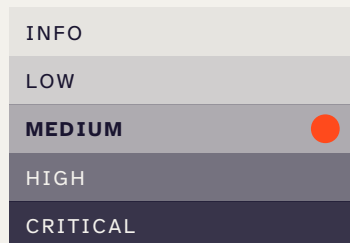
Finding 5 of 14

There are domains almost identical to the company's, ready to send and receive email

CVSS 3.1

5.4**MEDIUM**

DEPTH



AREA

brand

DOMAIN

Social

WHAT IS AT STAKE

A domain with one letter changed and working email is the classic tool of invoice fraud: the customer gets an email that seems to come from the company, from an almost identical address, with new bank details.

FINANCIAL EXPOSURE**Fake email fraud**

The typical loss is the amount of the diverted invoice or payment.

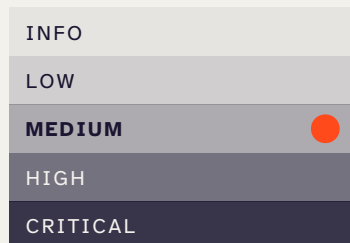
Finding 6 of 14

There are services open to the internet besides the website

CVSS 3.1

5.3**MEDIUM**

DEPTH



AREA

servers

DOMAIN

Server

WHAT IS AT STAKE

Each open service (remote access, databases, admin panels) is one more door that can be attacked by password or through a software flaw. Many automated attacks sweep the internet looking for exactly these ports.

03 · LOWER SEVERITY

Low and informational

LOW CVSS 3.7 Finding 7 of 14 domain · Domain

The domain's DNS answers are not signed (DNSSEC)

WHAT IS AT STAKE

Without a signature, an attacker who manages to poison an intermediate DNS server can send visitors or email to a server of their own. It is an uncommon attack, and turning DNSSEC on is usually an option at the domain provider.

LOW CVSS 3.7 Finding 8 of 14 email · Email

Email the company receives can travel without encryption

WHAT IS AT STAKE

Someone with access to the network the email crosses can force messages to travel without encryption and read them. It is a hard attack, but company email carries invoices, contracts and passwords.

LOW CVSS 3.1 Finding 9 of 14 website · Web

The website hands out cookies without the basic protections

WHAT IS AT STAKE

If one of those cookies identifies a user's session, a minor bug in the website is enough to steal it and get into their account.

LOW CVSS 3.1 Finding 10 of 14 website · Web

The website is missing its basic security headers

WHAT IS AT STAKE

They are not a flaw on their own, but without them a bug in the website (a badly validated form, a vulnerable plugin) becomes much easier to use against visitors.

INFO CVSS 0.0 Finding 11 of 14 domain · Domain

Nothing restricts who can issue certificates for the domain

WHAT IS AT STAKE

It is an extra layer: it lowers the chance that someone gets a valid certificate for the domain by fooling a careless authority.

INFO CVSS 0.0 Finding 12 of 14 email · Email

Nobody receives the reports on who uses the domain's name

WHAT IS AT STAKE

Without those reports the company does not find out if someone is sending email in its name, and has no data to tighten the policy without cutting off its own sending.

INFO CVSS 0.0 Finding 13 of 14 website · Web

The website announces which software and version it runs

WHAT IS AT STAKE

It is not a flaw, but it saves work for whoever hunts for websites running a vulnerable version to attack them in bulk.

INFO CVSS 0.0 Finding 14 of 14 website · Web

There is no published contact for reporting security flaws

WHAT IS AT STAKE

Whoever finds a problem and does not know whom to write to usually publishes it or drops it. With a clear contact, the company hears first.

04 · NEXT STEPS

What this analysis does not look at

This analysis reads only public data from taruma-pagos.example: it does not get into your website or your systems. What is inside is what an audit looks at, with your signed authorization:

US\$4,500

Dig

Your website and your servers tested from the inside: the login, the forms, the payments and what runs behind them.

lop.run/en/services/dig

US\$9,500

Rabbit Hole

Your whole platform: each customer's accounts and permissions, the APIs, the business logic and the cloud.

lop.run/en/services/rabbit-hole

from US\$15,000

Warren

Your whole company: besides the platform, the office network, the Wi-Fi, the email and whether your team falls for a scam.

lop.run/en/services/warren

US\$490

Sniff

Not sure which one you need? A specialist goes over this analysis with you for 30 minutes and tells you, at a fixed price. If you then hire an audit, it is credited.

lop.run/en/services/sniff

What you can do now

Free

Monitoring badge

We check your domain once a month, at no cost, and write to you only if something changed.

lop.run/en/services/#free

US\$449 per month

Ears + Lop

We watch your domain around the clock and a specialist confirms every alert before it reaches you and tells you what to do. This analysis found serious findings: with a person beside you, you do not depend on reading each alert yourself.

lop.run/en/services/ears-lop

US\$95 per hour (minimum US\$150)

Lop Fix

This report has 11 configuration fixes. If you would rather not do them yourself, we do them for you.

lop.run/en/services/lop-fix

LEADERSHIP BRIEF

Prepared for taruma- pagos.example.

This analysis read only public data from taruma-pagos.example on 2026-10-28. Nobody tested or touched your systems. If you want legal advice on these obligations, we can put you in touch with specialized lawyers.