



Example Company, Inc.

DOMAIN

empresa-ejemplo.example

DATE

October 2026

REFERENCE

NG-SAMPLE-001

SCOPE

Authorized external review, no exploits. Read-only cloud audit (AWS in this example; also Azure, Google Cloud and Oracle Cloud depending on the project).

1. Executive summary

2

Critical

5

High

8

Medium

100%

With evidence

Example Company's external surface has two critical findings worth addressing this week: employee credentials in a breach dataset and a backup bucket with public

read access. Both were verified with evidence and neither needed exploitation to be confirmed.

Behind them there are five high findings, mostly cloud configuration and TLS, and eight medium ones that improve overall posture without immediate urgency.

What to address first

THIS WEEK

Rotate the leaked credentials and close public access to the bucket (NG-01, NG-02).

30 DAYS

Reduce deployment role permissions, retire old TLS and protect the admin panel (NG-03 to NG-07).

90 DAYS

DNS hygiene, headers and encryption at rest (NG-08 to NG-15).

2. Scope and methodology

External review authorized in writing. Sources: public certificate records, exposed infrastructure search engines, breach datasets and active enumeration. Cloud audit with read-only access agreed in the scope (AWS in this example).

Every finding is tested before it is recorded. The report separates what was verified from what was observed and from indications.

Validation levels

Verified	Confirmed with reproducible evidence.
Observed	The signal was observed; impact still needs an authenticated test to confirm.

Indication Weak signal; listed apart and not counted as a finding.

3. Findings

ID	FINDING	SEVERITY	SOURCE	EVIDENCE	STATUS
NG - 01	Leaked credentials (infostealer)	CRIT	Breaches	verified record	Verified
NG - 02	Backup bucket with public read access	CRIT	Cloud AWS	public listing	Verified
NG - 03	Excessive IAM privileges	HIGH	AWS	IAM policy	Verified
NG - 04	Outdated TLS protocol	HIGH	Handshake	TLS version	Verified
NG - 05	Admin panel exposed with no visible MFA	HIGH	Live hosts	status 200 + login	Observed
NG - 06	Service access key not rotated in over a year	HIGH	AWS	credential report	Verified
NG - 07	Certificate close to expiring on a critical service	HIGH	Handshake	expiry date	Verified
NG - 08	Exposed development subdomain	MED	Live hosts	status 200	Verified
NG - 09	SPF softfail instead of hardfail	MED	DNS	dig TXT	Verified
NG - 10	DMARC in monitoring mode (p=none)	MED	DNS	dig TXT	Verified
NG - 11	Security headers missing (HSTS, CSP)	MED	Handshake	HTTP headers	Verified

ID	FINDING	SEVERITY	SOURCE	EVIDENCE	STATUS
NG - 12	Server version visible in the banner	MED	Live hosts	HTTP banner	Observed
NG - 13	Orphaned DNS records	MED	DNS	CNAME with no target	Verified
NG - 14	Admin port open to a wide range	MED	AWS	security group	Verified
NG - 15	Two volumes without encryption at rest	MED	AWS	EBS config	Verified

Findings in detail

NG-01

CRIT

Leaked credentials (infostealer)

IMPACT

With a valid employee credential, an attacker can reach services without going through any network defense.

RECOMMENDATION

- Rotate the password of the affected accounts and revoke active sessions.
- Enable MFA on every service the account can access.
- Review the user's device: the source is usually an infostealer on the endpoint.

EVIDENCE

```
dataset : breach-corpus (infostealer record)
account : a***@empresa-ejemplo.example
date    : matches the reported infection window
password: [redacted in this report]
```

VALIDATION

Verified: the dataset record matches the domain and the date. No service access was attempted.

Backup bucket with public read access

IMPACT

Backups can hold customer data and application secrets. Anyone on the Internet can list and download them.

RECOMMENDATION

- Block public access at the account level (S3 Block Public Access).
- Review access logs to learn whether someone else downloaded objects.
- Rotate any secret that lived in those backups.

EVIDENCE

```
$ curl -s https://backups-example.s3.amazonaws.com/ | head
<ListBucketResult>
  <Name>backups-example</Name>
  <Contents><Key>db/2026-09-30.sql.gz</Key>...
(public listing; no object was downloaded)
```

VALIDATION

Verified: the listing is visible without authentication. No content was downloaded.

NG-03

HIGH

Excessive IAM privileges

IMPACT

A role with admin permissions widens the damage of any compromised credential: the attacker inherits control of the account.

RECOMMENDATION

- Replace the policy with least-privilege permissions for deployments.
- Separate the deployment role from the runtime role.
- Enable alerts for unusual use of the role.

EVIDENCE

```
{  
  "RoleName": "app-deploy",  
  "Statement": [{ "Effect": "Allow", "Action": "*", "Resource": "*" }]  
}
```

VALIDATION

Verified: policy review with the read-only access agreed in the scope.

NG-04

HIGH

Outdated TLS protocol

IMPACT

Old TLS protocols have known weaknesses and may fail compliance requirements.

RECOMMENDATION

- Disable TLS 1.0 and 1.1; allow only TLS 1.2 and 1.3.
- Check that no legitimate client depends on the old protocol.

EVIDENCE

```
$ openssl s_client -connect portal.empresa-ejemplo.example:443 -tls1
Protocol  : TLSv1
Cipher    : ECDHE-RSA-AES256-SHA
Verify return code: 0 (ok)
```

VALIDATION

Verified: the server accepted the handshake over TLS 1.0.

NG-09

MED

SPF softfail instead of hardfail

IMPACT

With SPF in softfail, a spoofed email using the domain can still reach the inbox.

RECOMMENDATION

- Move SPF to -all once DMARC is on quarantine or reject.
- Publish DKIM for every legitimate sender.

EVIDENCE

```
$ dig +short TXT empresa-ejemplo.example
"v=spf1 include:_spf.vendor.example ~all"
```

VALIDATION

Verified: the public DNS record confirms it.

4. Remediation plan

Suggested order by real severity and effort. Dates are agreed in the debrief call.

THIS WEEK

- NG-01 Leaked credentials (infostealer)
- NG-02 Backup bucket with public read access

30 DAYS

- NG-03 Excessive IAM privileges
- NG-04 Outdated TLS protocol
- NG-05 Admin panel exposed with no visible MFA
- NG-06 Service access key not rotated in over a year
- NG-07 Certificate close to expiring on a critical service

90 DAYS

- NG-08 Exposed development subdomain
- NG-09 SPF softfail instead of hardfail
- NG-10 DMARC in monitoring mode (p=none)
- NG-11 Security headers missing (HSTS, CSP)
- NG-12 Server version visible in the banner
- NG-13 Orphaned DNS records
- NG-14 Admin port open to a wide range
- NG-15 Two volumes without encryption at rest

5. Notes

This document is an example with fictional data: the domain, addresses, accounts and results do not correspond to any real company.

A real report includes the full evidence for every finding, detailed remediation and a results session. Scope and deliverables are defined in the proposal.