TLP:GREEN

LEXFO

Audit report

Penetration test - AWS Config

External assets

MORPHO

Version 1.4 of 2023-05-25

TLP:GREEN

Document references

Document status

Version	Date	Status
V 1.4	2023-05-25	Document update

Traffic Light Protocol[1] (TLP) referential for information sharing:

TLP:RED = For the eyes and ears of individual recipients only, no further disclosure. Sources may use TLP:RED when information cannot be effectively acted upon without significant risk for the privacy, reputation, or operations of the organizations involved. Recipients may therefore not share TLP:RED information with anyone else. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting.

TLP:AMBER = Limited disclosure, recipients can only spread this on a need-to-know basis within their organization and its clients. Note that TLP:AMBER+STRICT restricts sharing to the organization only. Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm.

TLP:GREEN = Limited disclosure, recipients can spread this within their community. Sources may use TLP:GREEN when information is useful to increase awareness within their wider community. Recipients may share TLP:GREEN information with peers and partner organizations within their community, but not via publicly accessible channels. TLP:GREEN information may not be shared outside of the community. Note: when “community” is not defined, assume the cybersecurity/defense community.

TLP:CLEAR = Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

[1] Reference to the following document by FIRST: https://www.first.org/tlp/docs/tlp-a4.pdf

Table of contents

1 Introduction

1.1 Context and objectives

MORPHO wishes to ensure that the security of its external assets does not introduce vulnerabilities in its environment.

For this purpose, the **LEXFO** auditors carried out the necessary tests to:

- Assess the security of the elements included in the audit scope.
- Identify potential risks.
- Provide the recommendations for mitigation measures.
- Raise awareness among the actors (executives, managers, IT staff).

1.2 Organization

This audit was performed from May 3, 2023 to May 10, 2023.

The application analysis was divided into features in order to follow the end-to-end process and ensure vulnerability assessment could be done in all security mechanisms and protections.

First, our experts analyzed the application with a black-box approach, i.e. without knowing any login nor authentication information.

Then, they followed a white-box approach using the application code provided by **MORPHO**.

All tests were performed from **LEXFO**'s premises.

1.3 Scope and prerequisites

1.3.1 Scope

The audit scope included all of Morpho's external assets, namely the following resources (not exhaustive):

- All the applications and services deployed on morpho.xyz, morpho-labs.io, morpho.dev and its subdomains;
- The public GitHub projects of the following organizations: morpho-dao, morpho-org and morpho-labs;
- The private GitHub provided by Morpho (association).

1.4 Tools and methodology

LEXFO uses manual techniques during all security audits (information gathering, research and development, intrusion testing, etc.). Most of the tools are either freely available on the Internet -grabbed from the hacking community- or specifically developed for the mission, therefore included in the Appendix part of this report.

1.5 Referentials

Several international referentials prevailing in the area of application weaknesses were used:

- The OWASP Top 10 2021, which lists the most impacting vulnerabilities[2] for penetration tests;
- The CWE vulnerability database of MITRE[3];
- The independent vulnerability database of OSVDB.[4]

These referentials are widely established in the Web development area and acknowledged as such in contracts, security products and certification/qualification guides (example: PCI-DSS).

[2] https://owasp.org/Top10/
[3] https://cwe.mitre.org/data/definitions/699.html
[4] http://www.osvdb.org/

2 Synthesis

2.1 Vulnerability summary

8 vulnerabilities were found during the assessment, among which 2 with a medium risk.

The overall security level is ranked as improvable.

ID	Vulnerability	Risk	Status
V2	Default configuration of CloudTrail log	Medium	Proven
V8	AWS Config not enabled	Medium	Proven
V1	Exposed API keys	Low	Proven
V3	Weak password policy	Low	Proven
V4	Root Account Used Recently	Low	Proven
V5	Obsolete AWS access key	Low	Proven
V6	Misconfiguration of S3 Bucket	Low	Proven
V7	Misconfiguration of VPC	Low	Proven

2.2 Executive summary

No critical or high vulnerabilities were found on Morpho's exposed perimeter. Indeed, most of the accessible domains expose documentation (Gitbooks), decentralized applications (dApps without a backend) or redirect to other external services (Notion, Medium, etc.).

API keys for Infura and Alchemy services are present in the source code of some applications. However, this information is not sensitive and its exposure presents a minor risk. It is recommended to check that the protection measures for these API keys are properly implemented by referring to the documentation services provider.

Several positive observations were made during the audit:

- → The infrastructure is deployed on AWS and protected by CloudFront.
- → The application dependencies are up to date: Swagger UI 4.15.5 for the API, latest version of Discourse for the forum, etc.
- → The application code is minimal, tested and documented, which makes it easier to maintain and identify security vulnerabilities.

After analysis of the public projects of the GitHub organizations linked to Morpho, no sensitive data was found in the source code.

Regarding the configuration of the AWS tenant:

On the identity and access management section, various points were raised. The presence of inactive accounts and access keys (**V5**) and a weak password policy (**V3**) was observed.

The associated risk is however largely reduced by the MFA authentication required for all employees.

A recent use of the root account has been reported (**V4**) Lexfo reminds that the good practices are in favor of a minimal use of this account and of nominative and dedicated accounts.

Configuration reinforcements are to be implemented on the CloudTrail service in order to guarantee the confidentiality, integrity and traceability of stored data (**V2**).

The S3 buckets exposition are well managed by the teams but Lexfo recommends to activate Bucket Access Logging to sensitive buckets (**V6**).

1	Audited solution	8	Vulnerabilities	0	High ranked	2	Medium ranked

2.3 Strong points

During the assessment, the following strong points were encountered.

Title	Description
Secure protocols	User / server interactions are mediated by HTTPS / SFTP / SSH, which enforces communication security and reduces the risk of sensitive data being compromised by an attacker with an access to the network.
Good SSL / TLS configuration	The SSL / TLS certificate is at the state of the art and its configuration does not expose any known vulnerability or weakness in the protocol. This ensures secure user/server interactions.
Security headers	The presence of HTTP security headers protects the application against certain types of attack, including XSS.
Minimal attack surface	The audited server exposes a minimal attack surface to attackers by allowing access to the necessary ports only.
Web Application Firewall (WAF)	The Web Application Firewall (WAF) set before the applications mitigates the risk of compromise.
Unit and integration testing	Setting up unit and integration testing is a software development good practice in order to check that no regression has been inserted.
Usage of well-known frameworks	Using a well-known, regularly updated framework guarantees that the code has been put to the test and ensures a high security level. Most frontends are developed with client-side frameworks which makes it hard to find and exploit vulnerabilities in these components. By architecture, it is really rare to find a Cross-Site Scripting vulnerability in these components.
Documentation provided	The client provided useful documentation that greatly helped to fully understand the product.
Clean code	The code is clean and easily readable, which makes it easier to maintain and identify security vulnerabilities.
Limited set of features	The limited set of features available on the scope drastically reduces the attack surface. No unnecessary entry points were discovered, which is a good security practice.

Title	Description
Up-to-date components	The components and technologies in use are up-to-date and are not exposed to any known vulnerability.

3 Tests description

3.1 Discovery phase

3.1.1 Description

LEXFO's auditors simulate the actions of an attacker wishing to obtain a maximum of technical information on the internal network of the audit. This information may allow the attacker to discover a forgotten source code archive, displaying a vulnerable version of a technology, or simply to facilitate a future attack by targeting the different technologies discovered.

3.1.2 Tests

During this phase, the following security tests are performed (non-exhaustive listing):

- TCP/UDP scans;
- ICMP exchanges (Traceroute, Ping);
- Mask request;
- Timestamp;
- Network cartography;
- Detection of reverse proxies, WAF, load balancers.

3.2 Black-box phase

3.2.1 Description

LEXFO's auditors simulate the actions of an attacker wishing to attack the internal network without any knowledge of the network architecture. The only information known is the one obtained during the discovery phase.

3.2.2 Tests

During this phase, the following security tests are performed (non-exhaustive listing):

- HTTP methods;
- Banner and version grabbing;
- Resource listing;
- SSL configuration.

3.3 Code audit phase

3.3.1 Description

LEXFO auditors simulate the actions of an attacker wishing to obtain a maximum of technical information on the internal functioning of the application and the communication protocol used with its Web Service. This information may allow the attacker to discover a forgotten source code archive, displaying a vulnerable version of technology or simply to facilitate a future attack by targeting the different technologies discovered.

3.3.2 Tests

During this phase, the following security tests are performed (non-exhaustive listing):

- → Finding comments in the source code;
- → Finding calls of dangerous functions;
- → Etc.

Authentication analysis:

- → Finding possibilities for user listing;
- → Finding authentication bypass.

Authorization analysis:

- → Finding authorization bypass, privilege escalation, etc.

Analysis of business functionalities:

- → Consistency of results after data corruption between two steps during a process (client/server issues);
- → Analysis of the application behavior when sending inconsistent data.
- → Etc.

4 Matrix description

4.1 Vulnerability table

<table>
<tr><td>Vx</td><td colspan="2">Vulnerability</td><td>STATUS
(see below)</td><td>RISK
Risk level</td></tr>
<tr><td colspan="5">CONSEQUENCES
Description of the consequences related to the vulnerability.</td></tr>
<tr><td colspan="5">AFFECTED COMPONENT
List of the components affected by the vulnerability.</td></tr>
<tr><td colspan="5">MITIGATION
List of the recommendations provided to mitigate the issue.</td></tr>
<tr><td colspan="2">EXPLOITABILITY
(see below)</td><td>IMPACT
(see below)</td><td colspan="2">CORRECTION DIFFICULTY
(see below)</td></tr>
</table>

4.2 Metrics

Global security level (used in the executive summary)	
Excellent	**No vulnerability or only one low-risk vulnerability** was found on the audited scope because of the effective implementation of security mechanisms.
Acceptable	**Only low-risk vulnerabilities** were identified during the audit. The overall security level of the audited scope prevents even an experienced attacker from compromising the data.
Improvable	**One or more medium-risk vulnerabilities** were discovered during the audit. These vulnerabilities could be exploited by an experienced attacker wishing to damage the Client's image.
Insufficient	**One or more high-risk vulnerabilities and/or only one critical vulnerability** were identified during the audit. The impacts for the client may be important (data theft, brand image damage, etc.), but do not lead to the compromise of the audited scope.
Critical	**One or more critical vulnerabilities** were found, leading to a total compromise of the audited scope and/or with significant technical (service totally unavailable, breach of data confidentiality, etc.) or business (brand image or financial damages, etc.) impacts.

Status	
Proven	The presence of the vulnerability has been demonstrated.
To be confirmed	The presence of the vulnerability could not be proven. Checks should be performed by the Client.
Untested	The vulnerability has not been tested due to potential risks of denial of service, unavailability, etc.
Fixed	The vulnerability has been fixed.
Not fixed	The vulnerability has not been fixed. Checks should be performed by the Client.
Partially fixed	The vulnerability has been partially fixed. Checks should still be performed by the Client.

Correction difficulty	
Complex	Sharp computer skills, a lot of time or important financial resources are needed.
Moderate	Comprehensive computer knowledge, a little time and limited financial means are necessary.
Simple	Little knowledge, resources and time are required.

Impact	
Insignificant	The impacts can be overcome without difficulty.
Limited	The impacts can be overcome with some difficulties.
Important	The impacts can be overcome with serious difficulties.
Critical	The impacts are potentially insurmountable.

Exploitability	
Very difficult	Exploitation of unpublished vulnerabilities requiring security expertise of information systems and the development of specific and targeted tools.
Difficult	Exploitation of public vulnerabilities requiring security expertise of information systems and the development of simple tools.
Moderate	Exploitation requiring simple techniques and/or publicly available tools.
Easy	Trivial exploitation, without any specific tools.

Risk level (calculated according to exploitability and impact)	
Critical	Critical risk for the information system, requiring an immediate correction or imposing an immediate stop of the service.
High	Major risk on the information system, requiring a short-term correction.
Medium	Moderate risk on the information system, requiring a medium-term correction.
Low	Low risk on the information system, that may require a correction.

4.3 Risk computing

		Exploitability			
		Very difficult	Difficult	Moderate	Easy
Impact	Insignificant	Low	Low	Medium	High
	Limited	Low	Medium	Medium	High
	Important	Medium	High	High	Critical
	Critical	Medium	High	Critical	Critical

5 Information gathering

DNS zone transfer

Command

```
$ dnsrecon -t axfr -d morpho.xyz
```

Output

```
[*] Checking for Zone Transfer for morpho.xyz name servers
[*] Resolving SOA Record
[+]      SOA ns-558.awsdns-05.net 205.251.194.46
[+]      SOA ns-558.awsdns-05.net 2600:9000:5302:2e00::1
[*] Resolving NS Records
[*] NS Servers found:
[+]      NS ns-558.awsdns-05.net 205.251.194.46
[+]      NS ns-558.awsdns-05.net 2600:9000:5302:2e00::1
[+]      NS ns-112.awsdns-14.com 205.251.192.112
[+]      NS ns-112.awsdns-14.com 2600:9000:5300:7000::1
[+]      NS ns-1372.awsdns-43.org 205.251.197.92
[+]      NS ns-1372.awsdns-43.org 2600:9000:5305:5c00::1
[+]      NS ns-1997.awsdns-57.co.uk 205.251.199.205
[+]      NS ns-1997.awsdns-57.co.uk 2600:9000:5307:cd00::1
[*] Removing any duplicate NS server IP Addresses...
[*]
[*] Trying NS server 2600:9000:5305:5c00::1
[-] Zone Transfer Failed for 2600:9000:5305:5c00::1!
[-] Port 53 TCP is being filtered
[*]
[*] Trying NS server 2600:9000:5307:cd00::1
[-] Zone Transfer Failed for 2600:9000:5307:cd00::1!
[-] Port 53 TCP is being filtered
[*]
[*] Trying NS server 2600:9000:5302:2e00::1
[-] Zone Transfer Failed for 2600:9000:5302:2e00::1!
[-] Port 53 TCP is being filtered
[*]
[*] Trying NS server 205.251.199.205
[+] 205.251.199.205 Has port 53 TCP Open
[-] Zone Transfer Failed ([Errno 104] Connection reset by peer)
[*]
[*] Trying NS server 205.251.194.46
[+] 205.251.194.46 Has port 53 TCP Open
[-] Zone Transfer Failed ([Errno 104] Connection reset by peer)
[*]
[*] Trying NS server 205.251.197.92
[+] 205.251.197.92 Has port 53 TCP Open
[-] Zone Transfer Failed ([Errno 104] Connection reset by peer)
[*]
[*] Trying NS server 2600:9000:5300:7000::1
[-] Zone Transfer Failed for 2600:9000:5300:7000::1!
[-] Port 53 TCP is being filtered
[*]
[*] Trying NS server 205.251.192.112
[+] 205.251.192.112 Has port 53 TCP Open
[-] Zone Transfer Failed ([Errno 104] Connection reset by peer)
```

DNS zone transfer is not allowed, which reduces the possibility for an attacker to recover the content of the DNS server associated with the audited application. This is a good security practice.

TRACEROUTE

Command

```
$traceroute morpho.xyz
```

Output

```
traceroute to morpho.xyz (13.32.145.128), 30 hops max, 60 byte packets
 1  192.168.1.254 (192.168.1.254)  18.827 ms  18.747 ms  18.726 ms
 2  station9.multimania.isdnet.net (194.149.174.106)  16.578 ms  16.557 ms
16.540 ms
 3  station17.multimania.isdnet.net (194.149.174.114)  16.522 ms  16.504 ms
16.485 ms
 4  99.83.89.112 (99.83.89.112)  22.453 ms  22.424 ms  22.406 ms
 5  52.46.95.12 (52.46.95.12)  16.395 ms 52.46.95.36 (52.46.95.36)  16.381 ms
52.46.95.12 (52.46.95.12)  16.360 ms
 6  52.46.95.171 (52.46.95.171)  16.335 ms 52.46.95.169 (52.46.95.169)  4.022 ms
52.46.95.173 (52.46.95.173)  5.910 ms
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  * * *
12  server-13-32-145-128.cdg50.r.cloudfront.net (13.32.145.128)  5.212 ms  6.107
ms  6.088 ms
```

Command

```
$traceroute api.morpho.xyz
```

Output

```
traceroute to api.morpho.xyz (15.188.222.95), 30 hops max, 60 byte packets
 1  192.168.1.254 (192.168.1.254)  2.229 ms  3.116 ms  9.262 ms
 2  station11.multimania.isdnet.net (194.149.174.108)  14.429 ms  14.410 ms
14.391 ms
 3  station17.multimania.isdnet.net (194.149.174.114)  14.375 ms  14.357 ms
14.338 ms
 4  99.83.89.112 (99.83.89.112)  14.322 ms  14.304 ms  14.287 ms
 5  52.46.95.68 (52.46.95.68)  20.039 ms 52.46.95.12 (52.46.95.12)  14.351 ms *
 6  52.46.94.12 (52.46.94.12)  14.279 ms 52.46.94.2 (52.46.94.2)  5.562 ms
52.46.94.6 (52.46.94.6)  6.437 ms
 7  52.46.94.3 (52.46.94.3)  6.467 ms 52.46.94.47 (52.46.94.47)  6.348 ms
52.46.94.49 (52.46.94.49)  6.338 ms
 8  52.46.93.203 (52.46.93.203)  6.441 ms 52.46.93.199 (52.46.93.199)  6.433 ms
52.46.93.205 (52.46.93.205)  6.425 ms
 9  52.46.93.78 (52.46.93.78)  6.306 ms  6.300 ms 52.46.93.90 (52.46.93.90)
6.292 ms
10  * * *
11  * * *
12  * * *
13  ec2-15-188-222-95.eu-west-3.compute.amazonaws.com (15.188.222.95)  5.922 ms
5.904 ms  5.886 ms
```

Command

```
$traceroute vote.morpho.xyz
```

Output

```
traceroute to vote.morpho.xyz (143.244.56.51), 30 hops max, 60 byte packets
 1  192.168.1.254 (192.168.1.254)  5.667 ms  5.582 ms  5.548 ms
 2  station9.multimania.isdnet.net (194.149.174.106)  7.727 ms  7.699 ms  7.667
ms
 3  iliad.demarc.cogentco.com (149.11.175.170)  7.709 ms  7.681 ms  7.655 ms
 4  prs-b3-link.ip.twelve99.net (62.115.46.68)  12.369 ms  7.541 ms  12.318 ms
 5  prs-bb1-link.ip.twelve99.net (62.115.118.58)  7.547 ms prs-bb2-
link.ip.twelve99.net (62.115.118.62)  7.527 ms  7.507 ms
 6  prs-b1-link.ip.twelve99.net (62.115.125.171)  7.494 ms  7.991 ms  7.925 ms
 7  datacamp-ic-355852.ip.twelve99-cust.net (62.115.58.162)  7.897 ms  4.864 ms
4.801 ms
 8  vl223.par-itx5-dist-2.cdn77.com (185.156.45.109)  7.744 ms  7.724 ms  7.704
ms
 9  143-244-56-51.bunnyinfra.net (143.244.56.51)  7.641 ms  7.622 ms  7.603 ms
```

Command

```
$traceroute forum.morpho.xyz
```

Output

```
traceroute to forum.morpho.xyz (184.104.178.43), 30 hops max, 60 byte packets
 1  192.168.1.254 (192.168.1.254)  4.028 ms  3.968 ms  3.947 ms
 2  station11.multimania.isdnet.net (194.149.174.108)  6.434 ms  6.414 ms *
 3  * * station1.multimania.isdnet.net (194.149.174.98)  6.337 ms
 4  * * *
 5  * * *
 6  100ge0-32.core2.man1.he.net (72.52.92.197)  107.644 ms  98.419 ms hurricane-
ic-308792.ip.twelve99-cust.net (80.239.161.226)  98.384 ms
 7  router01.dub.discourse.cloud (184.104.178.254)  98.243 ms
router02.dub.discourse.cloud (184.104.178.255)  93.041 ms
router01.dub.discourse.cloud (184.104.178.254)  92.898 ms
 8  * router01.dub.discourse.cloud (184.104.178.254)  36.913 ms
router02.dub.discourse.cloud (184.104.178.255)  36.858 ms
```

The routes used by the network packets are easy to identify. Most of the exposed servers are deployed behind CloudFront and AWS.

Two domains redirect to servers deployed on bunnyinfra.net (vote.morpho.xyz) and discourse.cloud (forum.morpho.xyz).

No security issue was detected.

TCP scan

Command

```
$ nmap -sV -sC -O -T4 -n -Pn -iL domains.txt
```

Output

```
Nmap scan report for whitepaper.morpho.xyz (13.32.145.107)
Host is up (0.0058s latency).
Other addresses for whitepaper.morpho.xyz (not scanned):
2600:9000:20e1:200:16:9b82:8b00:93a1 2600:9000:20e1:0:16:9b82:8b00:93a1
2600:9000:20e1:4400:16:9b82:8b00:93a1 2600:9000:20e1:4000:16:9b82:8b00:93a1
2600:9000:20e1:1200:16:9b82:8b00:93a1 2600:9000:20e1:7e00:16:9b82:8b00:93a1
```

Command

```
2600:9000:20e1:400:16:9b82:8b00:93a1 2600:9000:20e1:fe00:16:9b82:8b00:93a1
13.32.145.128 13.32.145.59 13.32.145.3
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE  VERSION
80/tcp  open  http     Amazon CloudFront httpd
|_http-title: Did not follow redirect to https://whitepaper.morpho.xyz/
|_http-server-header: CloudFront
443/tcp open  ssl/http Amazon CloudFront httpd
|_http-title: Site doesn't have a title (application/pdf).
| ssl-cert: Subject: commonName=whitepaper.morpho.xyz
| Subject Alternative Name: DNS:whitepaper.morpho.xyz
| Not valid before: 2023-04-26T00:00:00
|_Not valid after:  2024-05-25T23:59:59
| http-server-header:
|   AmazonS3
|_  CloudFront
Warning: OSScan results may be unreliable because we could not find at least 1
open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): FreeBSD 11.X (88%)
OS CPE: cpe:/o:freebsd:freebsd:11.0
Aggressive OS guesses: FreeBSD 11.0-RELEASE (88%), FreeBSD 11.0-STABLE (88%),
FreeBSD 11.1-RELEASE (88%), FreeBSD 11.1-STABLE (88%)
No exact OS matches for host (test conditions non-ideal).

Nmap scan report for governance.morpho.xyz (18.164.52.21)
Host is up (0.0052s latency).
Other addresses for governance.morpho.xyz (not scanned):
2600:9000:2450:8e00:f:3567:b340:93a1 2600:9000:2450:8400:f:3567:b340:93a1
2600:9000:2450:c800:f:3567:b340:93a1 2600:9000:2450:b800:f:3567:b340:93a1
2600:9000:2450:4a00:f:3567:b340:93a1 2600:9000:2450:e200:f:3567:b340:93a1
2600:9000:2450:de00:f:3567:b340:93a1 2600:9000:2450:a600:f:3567:b340:93a1
18.164.52.96 18.164.52.124 18.164.52.61
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE  VERSION
80/tcp  open  http     Amazon CloudFront httpd
|_http-server-header: CloudFront
|_http-title: Did not follow redirect to https://governance.morpho.xyz/
443/tcp open  ssl/http Amazon CloudFront httpd
| http-server-header:
|   AmazonS3
|_  CloudFront
|_http-title: Site doesn't have a title (text/html).
| ssl-cert: Subject: commonName=governance.morpho.xyz
| Subject Alternative Name: DNS:governance.morpho.xyz
| Not valid before: 2022-12-22T00:00:00
|_Not valid after:  2024-01-20T23:59:59
Warning: OSScan results may be unreliable because we could not find at least 1
open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): FreeBSD 11.X (88%)
OS CPE: cpe:/o:freebsd:freebsd:11.0
Aggressive OS guesses: FreeBSD 11.0-RELEASE (88%), FreeBSD 11.0-STABLE (88%),
FreeBSD 11.1-RELEASE (88%), FreeBSD 11.1-STABLE (88%)
No exact OS matches for host (test conditions non-ideal).

Nmap scan report for design.morpho.xyz (13.249.9.107)
Host is up (0.0093s latency).
```

Command

```
Other addresses for design.morpho.xyz (not scanned):
2600:9000:2171:5c00:f:1710:2a80:93a1 2600:9000:2171:8000:f:1710:2a80:93a1
2600:9000:2171:7600:f:1710:2a80:93a1 2600:9000:2171:e600:f:1710:2a80:93a1
2600:9000:2171:e400:f:1710:2a80:93a1 2600:9000:2171:200:f:1710:2a80:93a1
2600:9000:2171:be00:f:1710:2a80:93a1 2600:9000:2171:b600:f:1710:2a80:93a1
13.249.9.24 13.249.9.129 13.249.9.72
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE  VERSION
80/tcp  open  http     Amazon CloudFront httpd
|_http-title: Did not follow redirect to https://design.morpho.xyz/
|_http-server-header: CloudFront
443/tcp open  ssl/http Amazon CloudFront httpd
| ssl-cert: Subject: commonName=design.morpho.xyz
| Subject Alternative Name: DNS:design.morpho.xyz
| Not valid before: 2023-02-23T00:00:00
|_Not valid after:  2023-10-05T23:59:59
| http-server-header:
|   AmazonS3
|_  CloudFront
|_http-title: Did not follow redirect to https://morpho-
labs.notion.site/c5a12580c6164b6a98f7f27edb2ec6e8?v=53047936a8194acfb450ee07efae
5d23/
Warning: OSScan results may be unreliable because we could not find at least 1
open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): FreeBSD 11.X|12.X (88%)
OS CPE: cpe:/o:freebsd:freebsd:11.1 cpe:/o:freebsd:freebsd:12.0
Aggressive OS guesses: FreeBSD 11.1-STABLE (88%), FreeBSD 12.0-RELEASE (88%),
FreeBSD 12.1-RELEASE (88%)
No exact OS matches for host (test conditions non-ideal).

Nmap scan report for doc.morpho.xyz (18.164.52.83)
Host is up (0.0061s latency).
Other addresses for doc.morpho.xyz (not scanned):
2600:9000:2450:8000:3:6cc5:9e40:93a1 2600:9000:2450:7e00:3:6cc5:9e40:93a1
2600:9000:2450:b200:3:6cc5:9e40:93a1 2600:9000:2450:9600:3:6cc5:9e40:93a1
2600:9000:2450:c800:3:6cc5:9e40:93a1 2600:9000:2450:7a00:3:6cc5:9e40:93a1
2600:9000:2450:0:3:6cc5:9e40:93a1 2600:9000:2450:aa00:3:6cc5:9e40:93a1
18.164.52.50 18.164.52.21 18.164.52.61
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE  VERSION
80/tcp  open  http     Amazon CloudFront httpd
|_http-title: Did not follow redirect to https://doc.morpho.xyz/
|_http-server-header: CloudFront
443/tcp open  ssl/http Amazon CloudFront httpd
| http-server-header:
|   AmazonS3
|_  CloudFront
| ssl-cert: Subject: commonName=documentation.morpho.xyz
| Subject Alternative Name: DNS:documentation.morpho.xyz, DNS:doc.morpho.xyz
| Not valid before: 2023-03-02T00:00:00
|_Not valid after:  2023-09-06T23:59:59
| http-title: Homepage - Morpho General Documentation
|_Requested resource was https://docs.morpho.xyz/start-here/homepage
Warning: OSScan results may be unreliable because we could not find at least 1
open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results
incomplete
```

Command

```
No OS matches for host

Nmap scan report for documentation.morpho.xyz (18.164.52.50)
Host is up (0.0066s latency).
Other addresses for documentation.morpho.xyz (not scanned):
2600:9000:2450:7a00:3:6cc5:9e40:93a1 2600:9000:2450:0:3:6cc5:9e40:93a1
2600:9000:2450:aa00:3:6cc5:9e40:93a1 2600:9000:2450:8000:3:6cc5:9e40:93a1
2600:9000:2450:7e00:3:6cc5:9e40:93a1 2600:9000:2450:b200:3:6cc5:9e40:93a1
2600:9000:2450:9600:3:6cc5:9e40:93a1 2600:9000:2450:c800:3:6cc5:9e40:93a1
18.164.52.21 18.164.52.61 18.164.52.83
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE  VERSION
80/tcp  open  http     Amazon CloudFront httpd
|_http-server-header: CloudFront
|_http-title: Did not follow redirect to https://documentation.morpho.xyz/
443/tcp open  ssl/http Amazon CloudFront httpd
| http-server-header:
|   AmazonS3
|_  CloudFront
| http-title: Homepage - Morpho General Documentation
|_Requested resource was https://docs.morpho.xyz/start-here/homepage
| ssl-cert: Subject: commonName=documentation.morpho.xyz
| Subject Alternative Name: DNS:documentation.morpho.xyz, DNS:doc.morpho.xyz
| Not valid before: 2023-03-02T00:00:00
|_Not valid after:  2023-09-06T23:59:59
Warning: OSScan results may be unreliable because we could not find at least 1
open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): FreeBSD 11.X|12.X (88%)
OS CPE: cpe:/o:freebsd:freebsd:11.1 cpe:/o:freebsd:freebsd:12.0
Aggressive OS guesses: FreeBSD 11.1-STABLE (88%), FreeBSD 12.0-RELEASE (88%),
FreeBSD 12.1-RELEASE (88%)
No exact OS matches for host (test conditions non-ideal).

Nmap scan report for app.morpho.xyz (52.222.174.30)
Host is up (0.0066s latency).
Other addresses for app.morpho.xyz (not scanned):
2600:9000:218d:ee00:14:424:dc40:93a1 2600:9000:218d:c00:14:424:dc40:93a1
2600:9000:218d:8c00:14:424:dc40:93a1 2600:9000:218d:e200:14:424:dc40:93a1
2600:9000:218d:6800:14:424:dc40:93a1 2600:9000:218d:5e00:14:424:dc40:93a1
2600:9000:218d:f200:14:424:dc40:93a1 2600:9000:218d:2400:14:424:dc40:93a1
52.222.174.37 52.222.174.111 52.222.174.19
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE  VERSION
80/tcp  open  http     Amazon CloudFront httpd
|_http-title: Did not follow redirect to https://app.morpho.xyz/
|_http-server-header: CloudFront
443/tcp open  ssl/http Amazon CloudFront httpd
|_http-title:  Hub | Morpho
| ssl-cert: Subject: commonName=app.morpho.xyz
| Subject Alternative Name: DNS:app.morpho.xyz
| Not valid before: 2023-04-24T00:00:00
|_Not valid after:  2024-05-22T23:59:59
| http-server-header:
|   AmazonS3
|_  CloudFront
Warning: OSScan results may be unreliable because we could not find at least 1
open and 1 closed port
```

Command

```
Device type: general purpose
Running (JUST GUESSING): FreeBSD 11.X|12.X (88%)
OS CPE: cpe:/o:freebsd:freebsd:11.0 cpe:/o:freebsd:freebsd:12.0
Aggressive OS guesses: FreeBSD 11.0-RELEASE (88%), FreeBSD 11.0-STABLE (88%),
FreeBSD 11.1-RELEASE (88%), FreeBSD 11.1-STABLE (88%), FreeBSD 12.0-RELEASE
(86%)
No exact OS matches for host (test conditions non-ideal).

Nmap scan report for ipfs.morpho.xyz (15.188.29.7)
Host is up (0.0060s latency).
Other addresses for ipfs.morpho.xyz (not scanned): 15.188.222.95 13.37.206.185
Not shown: 997 closed tcp ports (reset)
PORT    STATE    SERVICE   VERSION
25/tcp  filtered smtp
80/tcp  open     http      awselb/2.0
|_http-server-header: awselb/2.0
|_http-title: Did not follow redirect to https://ipfs.morpho.xyz:443/
| fingerprint-strings:
|   GetRequest, HTTPOptions:
|     HTTP/1.1 301 Moved Permanently
|     Server: awselb/2.0
|     Date: Wed, 03 May 2023 12:56:54 GMT
|     Content-Type: text/html
|     Content-Length: 134
|     Connection: close
|     Location: https://morpho-alb-274421675.eu-west-3.elb.amazonaws.com:443/
|     <html>
|     <head><title>301 Moved Permanently</title></head>
|     <body>
|     <center><h1>301 Moved Permanently</h1></center>
|     </body>
|     </html>
443/tcp open     ssl/https awselb/2.0
| tls-nextprotoneg:
|   h2
|_  http/1.1
|_http-title: Site doesn't have a title (text/plain; charset=utf-8).
|_ssl-date: TLS randomness does not represent time
|_http-server-header: awselb/2.0
| ssl-cert: Subject: commonName=ipfs.morpho.xyz
| Subject Alternative Name: DNS:ipfs.morpho.xyz
| Not valid before: 2023-03-13T00:00:00
|_Not valid after:  2024-04-10T23:59:59
| tls-alpn:
|   h2
|_  http/1.1
Aggressive OS guesses: Linux 2.6.32 - 3.13 (93%), Linux 2.6.32 (90%), Linux 3.2
- 4.9 (90%), Linux 2.6.32 - 3.10 (90%), HP P2000 G3 NAS device (89%), Linux 5.1
(89%), Linux 5.0 - 5.4 (89%), Ubiquiti Pico Station WAP (AirOS 5.2.6) (89%),
Linux 2.6.32 - 3.1 (89%), Linux 5.0 (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 15 hops

Nmap scan report for forum.morpho.xyz (184.104.178.43)
Host is up (0.024s latency).
Other addresses for forum.morpho.xyz (not scanned): 2602:fd3f:1:ff01::2b
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE  SERVICE   VERSION
```

Command

```
22/tcp   open   ssh       OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)
80/tcp   open   http
| fingerprint-strings:
|   GetRequest, HTTPOptions:
|     HTTP/1.1 404 Not Found
|     cache-control: no-cache
|     content-length: 1427
|     content-type: text/html
|     cdck-proxy-id: app-router-tiehunter01.dub1
|     cdck-proxy-id: app-balancer-tieinterceptor1b.dub1
|     connection: close
|     <html>
|     <head>
|     <title>Site Not Found - Discourse</title>
|     <link href="https://fonts.googleapis.com/css?family=Open+Sans:300,600,700"
rel="stylesheet" type="text/css">
|     <style>
|     body {
|     font-family: 'Open Sans',Arial,sans-serif;
|     background-color: rgb(231,238,247);
|     background-image: url('https://discourse-cdn.s3.amazonaws.com/bg.jpg');
|     background-repeat: repeat;
|     background-position: left top;
|     padding-bottom: 3em;
|     #logo {
|     width: 80%;
|     .content {
|     width: 60%;
|     max-width: 600px;
|     margin: 1em auto;
|     background-color: white;
|     padding: 1em;
|_    box-shadow: 0 5px 10px rgba(0,0,0,0.2);
|_http-title: Did not follow redirect to https://forum.morpho.xyz/
443/tcp  open   ssl/https nginx
|_http-server-header: nginx
|_ssl-date: TLS randomness does not represent time
| http-robots.txt: 17 disallowed entries (15 shown)
| / /admin/ /auth/ /assets/browser-update*.js /email/
| /session /user-api-key /*?api_key* /*?*api_key* /badges /u/ /my
|_/search /tag/*/l /g
| fingerprint-strings:
|   GetRequest, HTTPOptions:
|     HTTP/1.1 404 Not Found
|     cache-control: no-cache
|     content-length: 1427
|     content-type: text/html
|     cdck-proxy-id: app-router-tiehunter01.dub1
|     cdck-proxy-id: app-balancer-tieinterceptor1b.dub1
|     connection: close
|     <html>
|     <head>
|     <title>Site Not Found - Discourse</title>
|     <link href="https://fonts.googleapis.com/css?family=Open+Sans:300,600,700"
rel="stylesheet" type="text/css">
|     <style>
|     body {
|     font-family: 'Open Sans',Arial,sans-serif;
```

Command

```
|     background-color: rgb(231,238,247);
|     background-image: url('https://discourse-cdn.s3.amazonaws.com/bg.jpg');
|     background-repeat: repeat;
|     background-position: left top;
|     padding-bottom: 3em;
|     #logo {
|     width: 80%;
|     .content {
|     width: 60%;
|     max-width: 600px;
|     margin: 1em auto;
|     background-color: white;
|     padding: 1em;
|_    box-shadow: 0 5px 10px rgba(0,0,0,0.2);
|_http-title: Site doesn't have a title (text/html; charset=utf-8).
| ssl-cert: Subject: commonName=forum.morpho.xyz
| Subject Alternative Name: DNS:forum.morpho.xyz
| Not valid before: 2023-03-19T00:00:07
|_Not valid after:  2023-06-17T00:00:06
5000/tcp closed upnp
Aggressive OS guesses: Linux 2.6.32 - 3.13 (95%), Linux 2.6.32 (92%), Linux 3.2
- 4.9 (92%), Linux 2.6.32 - 3.10 (92%), HP P2000 G3 NAS device (91%), Infomir
MAG-250 set-top box (91%), Ubiquiti AirMax NanoStation WAP (Linux 2.6.32) (91%),
Linux 5.4 (90%), Linux 2.6.23 - 2.6.38 (89%), Linux 3.2 - 3.8 (89%)
No exact OS matches for host (test conditions non-ideal).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for blog.morpho.xyz (99.86.91.16)
Host is up (0.0065s latency).
Other addresses for blog.morpho.xyz (not scanned):
2600:9000:2117:e00:1:a04f:b400:93a1 2600:9000:2117:a800:1:a04f:b400:93a1
2600:9000:2117:3e00:1:a04f:b400:93a1 2600:9000:2117:7e00:1:a04f:b400:93a1
2600:9000:2117:4e00:1:a04f:b400:93a1 2600:9000:2117:9400:1:a04f:b400:93a1
2600:9000:2117:ba00:1:a04f:b400:93a1 2600:9000:2117:2a00:1:a04f:b400:93a1
99.86.91.46 99.86.91.59 99.86.91.33
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE  VERSION
80/tcp  open  http     Amazon CloudFront httpd
|_http-title: Did not follow redirect to https://blog.morpho.xyz/
|_http-server-header: CloudFront
443/tcp open  ssl/http Amazon CloudFront httpd
|_http-title: Did not follow redirect to https://medium.com/morpho-labs/
| ssl-cert: Subject: commonName=blog.morpho.xyz
| Subject Alternative Name: DNS:blog.morpho.xyz
| Not valid before: 2023-02-22T00:00:00
|_Not valid after:  2023-10-04T23:59:59
| http-server-header:
|   AmazonS3
|_  CloudFront
Warning: OSScan results may be unreliable because we could not find at least 1
open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): FreeBSD 11.X|12.X (88%)
OS CPE: cpe:/o:freebsd:freebsd:11.1 cpe:/o:freebsd:freebsd:12.0
Aggressive OS guesses: FreeBSD 11.1-RELEASE (88%), FreeBSD 11.0-RELEASE (86%),
FreeBSD 11.1-STABLE (86%), FreeBSD 12.0-RELEASE (86%)
No exact OS matches for host (test conditions non-ideal).
```

Command

```
Nmap scan report for cdn.morpho.xyz (52.222.174.5)
Host is up (0.0069s latency).
Other addresses for cdn.morpho.xyz (not scanned):
2600:9000:218d:9800:0:91cc:b5c0:93a1 2600:9000:218d:a400:0:91cc:b5c0:93a1
2600:9000:218d:5e00:0:91cc:b5c0:93a1 2600:9000:218d:2800:0:91cc:b5c0:93a1
2600:9000:218d:9400:0:91cc:b5c0:93a1 2600:9000:218d:4000:0:91cc:b5c0:93a1
2600:9000:218d:ca00:0:91cc:b5c0:93a1 2600:9000:218d:c800:0:91cc:b5c0:93a1
52.222.174.129 52.222.174.15 52.222.174.63
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE  VERSION
80/tcp  open  http     Amazon CloudFront httpd
|_http-server-header: CloudFront
|_http-title: Did not follow redirect to https://cdn.morpho.xyz/
443/tcp open  ssl/http Amazon CloudFront httpd
| ssl-cert: Subject: commonName=cdn.morpho.best
| Subject Alternative Name: DNS:cdn.morpho.best, DNS:cdn.morpho.xyz
| Not valid before: 2023-04-26T00:00:00
|_Not valid after:  2024-05-25T23:59:59
|_http-title: Site doesn't have a title (application/xml).
| http-server-header:
|   AmazonS3
|_  CloudFront
Warning: OSScan results may be unreliable because we could not find at least 1
open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): FreeBSD 11.X|12.X (88%)
OS CPE: cpe:/o:freebsd:freebsd:11.1 cpe:/o:freebsd:freebsd:12.0
Aggressive OS guesses: FreeBSD 11.1-STABLE (88%), FreeBSD 12.0-RELEASE (88%),
FreeBSD 12.1-RELEASE (88%)
No exact OS matches for host (test conditions non-ideal).

Nmap scan report for docs.morpho.xyz (104.18.3.117)
Host is up (0.0064s latency).
Other addresses for docs.morpho.xyz (not scanned): 2606:4700::6812:275
2606:4700::6812:375 104.18.2.117
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE  VERSION
80/tcp   open  http     Cloudflare http proxy
|_http-server-header: cloudflare
|_http-title: Did not follow redirect to https://docs.morpho.xyz/
443/tcp  open  ssl/http Cloudflare http proxy
| ssl-cert: Subject: commonName=docs.morpho.xyz
| Subject Alternative Name: DNS:docs.morpho.xyz
| Not valid before: 2023-03-09T19:46:25
|_Not valid after:  2023-06-07T19:46:24
| http-title: Homepage - Morpho General Documentation
|_Requested resource was /start-here/homepage
|_http-server-header: cloudflare
8080/tcp open  http     Cloudflare http proxy
|_http-title: Did not follow redirect to https://docs.morpho.xyz:8080/
|_http-server-header: cloudflare
8443/tcp open  ssl/http Cloudflare http proxy
| http-title: Homepage - Morpho General Documentation
|_Requested resource was /start-here/homepage
| ssl-cert: Subject: commonName=docs.morpho.xyz
| Subject Alternative Name: DNS:docs.morpho.xyz
| Not valid before: 2023-03-09T19:46:25
|_Not valid after:  2023-06-07T19:46:24
```

Command

```
|_http-server-header: cloudflare
Warning: OSScan results may be unreliable because we could not find at least 1
open and 1 closed port
Aggressive OS guesses: Crestron XPanel control system (91%), ASUS RT-N56U WAP
(Linux 3.4) (89%), Linux 3.1 (89%), Linux 3.16 (89%), Linux 3.2 (89%), AXIS 210A
or 211 Network Camera (Linux 2.6.17) (88%), HP P2000 G3 NAS device (88%), Linux
4.15 - 5.6 (87%), Linux 5.0 (87%), Linux 5.0 - 5.4 (87%)
No exact OS matches for host (test conditions non-ideal).

Nmap scan report for gov.morpho.xyz (13.249.9.108)
Host is up (0.0068s latency).
Other addresses for gov.morpho.xyz (not scanned):
2600:9000:2171:e000:d:d1ee:b080:93a1 2600:9000:2171:4a00:d:d1ee:b080:93a1
2600:9000:2171:4400:d:d1ee:b080:93a1 2600:9000:2171:8c00:d:d1ee:b080:93a1
2600:9000:2171:b800:d:d1ee:b080:93a1 2600:9000:2171:5a00:d:d1ee:b080:93a1
2600:9000:2171:8000:d:d1ee:b080:93a1 2600:9000:2171:8400:d:d1ee:b080:93a1
13.249.9.64 13.249.9.107 13.249.9.35
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE  VERSION
80/tcp  open  http     Amazon CloudFront httpd
|_http-title: Did not follow redirect to https://gov.morpho.xyz/
|_http-server-header: CloudFront
443/tcp open  ssl/http Amazon CloudFront httpd
| http-title:  Governance | Morpho
|_Requested resource was https://governance.morpho.xyz/
| ssl-cert: Subject: commonName=gov.morpho.xyz
| Subject Alternative Name: DNS:gov.morpho.xyz, DNS:governance.morpho.xyz
| Not valid before: 2023-03-01T00:00:00
|_Not valid after:  2023-09-06T23:59:59
| http-server-header:
|   AmazonS3
|_  CloudFront
Warning: OSScan results may be unreliable because we could not find at least 1
open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): FreeBSD 11.X|12.X (88%)
OS CPE: cpe:/o:freebsd:freebsd:11.1 cpe:/o:freebsd:freebsd:12.0
Aggressive OS guesses: FreeBSD 11.1-RELEASE (88%), FreeBSD 11.0-RELEASE (86%),
FreeBSD 11.1-STABLE (86%), FreeBSD 12.0-RELEASE (86%)
No exact OS matches for host (test conditions non-ideal).

Nmap scan report for www.morpho.xyz (13.32.145.128)
Host is up (0.0096s latency).
Other addresses for www.morpho.xyz (not scanned):
2600:9000:20e1:f600:12:7d09:e080:93a1 2600:9000:20e1:ba00:12:7d09:e080:93a1
2600:9000:20e1:de00:12:7d09:e080:93a1 2600:9000:20e1:6400:12:7d09:e080:93a1
2600:9000:20e1:7000:12:7d09:e080:93a1 2600:9000:20e1:ac00:12:7d09:e080:93a1
2600:9000:20e1:4a00:12:7d09:e080:93a1 2600:9000:20e1:5800:12:7d09:e080:93a1
13.32.145.116 13.32.145.29 13.32.145.109
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE  VERSION
80/tcp  open  http     Amazon CloudFront httpd
|_http-server-header: CloudFront
|_http-title: Did not follow redirect to https://www.morpho.xyz/
443/tcp open  ssl/http Amazon CloudFront httpd
| http-server-header:
|   AmazonS3
|_  CloudFront
```

Command

```
|_http-title: Morpho | Improving APY
| ssl-cert: Subject: commonName=*.morpho.xyz
| Subject Alternative Name: DNS:*.morpho.xyz, DNS:morpho.xyz
| Not valid before: 2023-02-23T00:00:00
|_Not valid after:  2023-08-10T23:59:59
Warning: OSScan results may be unreliable because we could not find at least 1
open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): FreeBSD 11.X (88%)
OS CPE: cpe:/o:freebsd:freebsd:11.0
Aggressive OS guesses: FreeBSD 11.0-RELEASE (88%), FreeBSD 11.0-STABLE (88%),
FreeBSD 11.1-RELEASE (88%), FreeBSD 11.1-STABLE (88%)
No exact OS matches for host (test conditions non-ideal).

Nmap scan report for job.morpho.xyz (52.222.174.100)
Host is up (0.0075s latency).
Other addresses for job.morpho.xyz (not scanned):
2600:9000:218d:bc00:1:bf30:e140:93a1 2600:9000:218d:c400:1:bf30:e140:93a1
2600:9000:218d:ce00:1:bf30:e140:93a1 2600:9000:218d:da00:1:bf30:e140:93a1
2600:9000:218d:2800:1:bf30:e140:93a1 2600:9000:218d:ba00:1:bf30:e140:93a1
2600:9000:218d:7c00:1:bf30:e140:93a1 2600:9000:218d:200:1:bf30:e140:93a1
52.222.174.101 52.222.174.52 52.222.174.21
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE  VERSION
80/tcp  open  http     Amazon CloudFront httpd
|_http-title: Did not follow redirect to https://job.morpho.xyz/
|_http-server-header: CloudFront
443/tcp open  ssl/http Amazon CloudFront httpd
| ssl-cert: Subject: commonName=jobs.morpho.xyz
| Subject Alternative Name: DNS:jobs.morpho.xyz, DNS:job.morpho.xyz
| Not valid before: 2023-02-24T00:00:00
|_Not valid after:  2023-09-06T23:59:59
|_http-title: Did not follow redirect to https://morpho-labs.notion.site/Morpho-
s-Open-Positions-e56ee0ec4e17438596ff7d573e5737e2/
| http-server-header:
|   AmazonS3
|_  CloudFront
Warning: OSScan results may be unreliable because we could not find at least 1
open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): FreeBSD 11.X (88%)
OS CPE: cpe:/o:freebsd:freebsd:11.0
Aggressive OS guesses: FreeBSD 11.0-RELEASE (88%), FreeBSD 11.0-STABLE (88%),
FreeBSD 11.1-RELEASE (88%), FreeBSD 11.1-STABLE (88%)
No exact OS matches for host (test conditions non-ideal).

Nmap scan report for developers.morpho.xyz (143.204.231.44)
Host is up (0.0066s latency).
Other addresses for developers.morpho.xyz (not scanned):
2600:9000:2113:f200:12:8639:6740:93a1 2600:9000:2113:200:12:8639:6740:93a1
2600:9000:2113:ea00:12:8639:6740:93a1 2600:9000:2113:e200:12:8639:6740:93a1
2600:9000:2113:2e00:12:8639:6740:93a1 2600:9000:2113:1a00:12:8639:6740:93a1
2600:9000:2113:fc00:12:8639:6740:93a1 2600:9000:2113:6e00:12:8639:6740:93a1
143.204.231.79 143.204.231.53 143.204.231.98
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE  VERSION
80/tcp  open  http     Amazon CloudFront httpd
|_http-server-header: CloudFront
```

Command

```
|_http-title: Did not follow redirect to https://developers.morpho.xyz/
443/tcp open  ssl/http Amazon CloudFront httpd
| http-server-header: 
|   AmazonS3
|_  CloudFront
| ssl-cert: Subject: commonName=developers.morpho.xyz
| Subject Alternative Name: DNS:developers.morpho.xyz
| Not valid before: 2023-03-06T00:00:00
|_Not valid after:  2024-04-03T23:59:59
|_http-title: Home
Warning: OSScan results may be unreliable because we could not find at least 1
open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): FreeBSD 11.X (88%)
OS CPE: cpe:/o:freebsd:freebsd:11.0
Aggressive OS guesses: FreeBSD 11.0-RELEASE (88%), FreeBSD 11.0-STABLE (88%),
FreeBSD 11.1-RELEASE (88%), FreeBSD 11.1-STABLE (88%)
No exact OS matches for host (test conditions non-ideal).

Nmap scan report for developer.morpho.xyz (18.155.129.37)
Host is up (0.0091s latency).
Other addresses for developer.morpho.xyz (not scanned):
2600:9000:244f:9a00:1f:a6f:5c80:93a1 2600:9000:244f:4800:1f:a6f:5c80:93a1
2600:9000:244f:a000:1f:a6f:5c80:93a1 2600:9000:244f:5000:1f:a6f:5c80:93a1
2600:9000:244f:8c00:1f:a6f:5c80:93a1 2600:9000:244f:ee00:1f:a6f:5c80:93a1
2600:9000:244f:ec00:1f:a6f:5c80:93a1 2600:9000:244f:6600:1f:a6f:5c80:93a1
18.155.129.77 18.155.129.104 18.155.129.92
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE  VERSION
80/tcp  open  http     Amazon CloudFront httpd
|_http-server-header: CloudFront
|_http-title: Did not follow redirect to https://developer.morpho.xyz/
443/tcp open  ssl/http Amazon CloudFront httpd
| http-title: Home
|_Requested resource was https://developers.morpho.xyz/
| ssl-cert: Subject: commonName=developer.morpho.xyz
| Subject Alternative Name: DNS:developer.morpho.xyz, DNS:dev.morpho.xyz,
DNS:devs.morpho.xyz
| Not valid before: 2023-02-21T00:00:00
|_Not valid after:  2023-09-06T23:59:59
| http-server-header: 
|   AmazonS3
|_  CloudFront
Warning: OSScan results may be unreliable because we could not find at least 1
open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): FreeBSD 11.X|12.X (88%)
OS CPE: cpe:/o:freebsd:freebsd:11.1 cpe:/o:freebsd:freebsd:12.0
Aggressive OS guesses: FreeBSD 11.1-STABLE (88%), FreeBSD 12.0-RELEASE (88%),
FreeBSD 12.1-RELEASE (88%)
No exact OS matches for host (test conditions non-ideal).

Nmap scan report for dev.morpho.xyz (18.155.129.77)
Host is up (0.0064s latency).
Other addresses for dev.morpho.xyz (not scanned):
2600:9000:244f:8c00:1f:a6f:5c80:93a1 2600:9000:244f:ee00:1f:a6f:5c80:93a1
2600:9000:244f:ec00:1f:a6f:5c80:93a1 2600:9000:244f:6600:1f:a6f:5c80:93a1
2600:9000:244f:9a00:1f:a6f:5c80:93a1 2600:9000:244f:4800:1f:a6f:5c80:93a1
```

Command

```
2600:9000:244f:a000:1f:a6f:5c80:93a1 2600:9000:244f:5000:1f:a6f:5c80:93a1
18.155.129.104 18.155.129.92 18.155.129.37
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE  VERSION
80/tcp  open  http     Amazon CloudFront httpd
|_http-title: Did not follow redirect to https://dev.morpho.xyz/
|_http-server-header: CloudFront
443/tcp open  ssl/http Amazon CloudFront httpd
| http-title: Home
|_Requested resource was https://developers.morpho.xyz/
| ssl-cert: Subject: commonName=developer.morpho.xyz
| Subject Alternative Name: DNS:developer.morpho.xyz, DNS:dev.morpho.xyz,
DNS:devs.morpho.xyz
| Not valid before: 2023-02-21T00:00:00
|_Not valid after:  2023-09-06T23:59:59
| http-server-header:
|   AmazonS3
|_  CloudFront
Warning: OSScan results may be unreliable because we could not find at least 1
open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): FreeBSD 11.X|12.X (88%)
OS CPE: cpe:/o:freebsd:freebsd:11.0 cpe:/o:freebsd:freebsd:12.0
Aggressive OS guesses: FreeBSD 11.0-STABLE (88%), FreeBSD 11.1-STABLE (88%),
FreeBSD 11.0-RELEASE (86%), FreeBSD 11.1-RELEASE (86%), FreeBSD 12.0-RELEASE
(86%)
No exact OS matches for host (test conditions non-ideal).

Nmap scan report for vote.morpho.xyz (143.244.56.51)
Host is up (0.0045s latency).
Other addresses for vote.morpho.xyz (not scanned): 2400:52e0:1e02::1074:1
Not shown: 974 closed tcp ports (reset)
PORT     STATE    SERVICE       VERSION
22/tcp   open     ssh           OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey:
|   3072 b4ad1fd903b24d1ef7b13a3e7b7a8fb0 (RSA)
|   256 e50375514d75da412d876d39598746a0 (ECDSA)
|_  256 58f37b54dc34e0da13b8fe8e20fb0a81 (ED25519)
25/tcp   filtered smtp
80/tcp   open     http          nginx
|_http-title: Snapshot
|_http-server-header: BunnyCDN-FR1-1074
|_http-cors: GET
443/tcp  open     ssl/http      nginx
| tls-alpn:
|   h2
|   http/1.1
|   http/1.0
|_  http/0.9
|_http-server-header: BunnyCDN-FR1-1074
| ssl-cert: Subject: commonName=vote.morpho.xyz
| Subject Alternative Name: DNS:vote.morpho.xyz
| Not valid before: 2023-04-22T12:11:11
|_Not valid after:  2023-07-21T12:11:10
|_ssl-date: TLS randomness does not represent time
|_http-title: Snapshot
|_http-cors: GET
```

Command

```
1935/tcp open     ssl/http       nginx
|_ssl-date: TLS randomness does not represent time
|_http-title: Site doesn't have a title (application/octet-stream).
| tls-alpn:
|   http/1.1
|   http/1.0
|_  http/0.9
| ssl-cert: Subject: commonName=vote.morpho.xyz
| Subject Alternative Name: DNS:vote.morpho.xyz
| Not valid before: 2023-04-22T12:11:11
|_Not valid after:  2023-07-21T12:11:10
6000/tcp open     http           nginx
|_http-title: 403 Forbidden
6001/tcp open     http           nginx
|_http-title: 403 Forbidden
6002/tcp open     http           nginx
|_http-title: 403 Forbidden
6003/tcp open     http           nginx
|_http-title: 403 Forbidden
6004/tcp open     http           nginx
|_http-title: 403 Forbidden
6005/tcp open     http           nginx
|_http-title: 403 Forbidden
6006/tcp open     http           nginx
|_http-title: 403 Forbidden
6007/tcp open     http           nginx
|_http-title: 403 Forbidden
6009/tcp open     http           nginx
|_http-title: 403 Forbidden
7000/tcp open     http           nginx
|_http-title: 403 Forbidden
7001/tcp open     http           nginx
|_http-title: 403 Forbidden
7002/tcp open     http           nginx
|_http-title: 403 Forbidden
7004/tcp open     http           nginx
|_http-title: 403 Forbidden
7007/tcp open     http           nginx
|_http-title: 403 Forbidden
7019/tcp open     http           nginx
|_http-title: 403 Forbidden
8082/tcp open     http           nginx
|_http-title: 403 Forbidden
8084/tcp open     http           nginx
|_http-title: 403 Forbidden
8085/tcp open     http           nginx
|_http-title: 403 Forbidden
8100/tcp open     xprint-server?
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.1 400 Bad Request
|     Connection: close
|     Content-Type: application/json; charset=utf-8
|     Date: Wed, 03 May 2023 12:57:37 GMT
|     Cache-Control: no-cache
|     {"status":400,"error":"Invalid Content-Length header, the body should send
at least one byte"}
|   GetRequest, HTTPOptions:
```

Command

```
|     HTTP/1.1 400 Bad Request
|     Connection: close
|     Content-Type: application/json; charset=utf-8
|     Date: Wed, 03 May 2023 12:57:11 GMT
|     Cache-Control: no-cache
|     {"status":400,"error":"Invalid Content-Length header, the body should send
at least one byte"}
|   Help, SSLSessionReq, TerminalServerCookie:
|     HTTP/1.1 400 Bad Request
|     Content-Length: 0
|     Connection: close
|     Date: Wed, 03 May 2023 12:57:26 GMT
|   Kerberos, TLSSessionReq:
|     HTTP/1.1 400 Bad Request
|     Content-Length: 0
|     Connection: close
|     Date: Wed, 03 May 2023 12:57:27 GMT
|   RTSPRequest:
|     HTTP/1.1 505 HTTP Version Not Supported
|     Content-Length: 0
|     Connection: close
|_    Date: Wed, 03 May 2023 12:57:11 GMT
8180/tcp open     unknown
|_http-title: BunnyCDN - Node FR1-1074
|_http-trane-info: Problem with XML parsing of /evox/about
| fingerprint-strings:
|   GetRequest, HTTPOptions:
|     HTTP/1.1 500 Internal Server Error
|     Connection: close
|     Content-Type: text/html
|     Date: Wed, 03 May 2023 12:57:11 GMT
|     Cache-Control: no-cache
|     ErrorCode: 113
|_    <html><head><title>500 Internal Server Error</title><link
href='//fonts.googleapis.com/css?family=Rubik:300,400,500' rel='stylesheet'
type='text/css'><style>html, body { width: 100%; margin: 0; padding: 0; text-
align: center; font-family: 'Rubik'; background-image:
url('data:image/svg+xml;base64,PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiP
z4KPHN2ZyB3aWR0aD0iMjg4MHB4IiBoZWlnaHQ9IjE0MjRweCIgdmlld0JveD0iMCAwIDI4ODAgMTQyN
CIgdmVyc2lvbj0iMS4xIiB4bWxucz0iaHR0cDovL3d3dy53My5vcmcvMjAwMC9zdmciIHhtbG5zOnhsa
W5rPSJodHRwOi8vd3d3LnczLm9yZy8xOTk5L3hsaW5rIj4KICAgIDxkZWZzPgogICAgICAgIDxyYWRpY
WxHcmFkaWVudCBjeD0iNDguNDU0MDQyMiUiIGN5PSIyNy4wMTE5NjQ1JSIgZng9IjQ4LjQ1NDA0MjIlI
iBmeT0iMjcuMDExOTY0NSUiIHI9IjcwLjg3MDg1MTQlIiBncmFkaWVudFRyYW5zZm9ybT0idHJ
8181/tcp open     intermapper?
Aggressive OS guesses: FreeBSD 12.0-RELEASE (89%), Linux 3.16 (88%), ASUS RT-
N56U WAP (Linux 3.4) (87%), Linux 3.1 (87%), Linux 3.2 (87%), Linux 2.6.23 -
2.6.38 (87%), Linux 3.2 - 3.8 (87%), Linux 3.5 (87%), AXIS 210A or 211 Network
Camera (Linux 2.6.17) (87%), DD-WRT v24-sp1 (Linux 2.4.36) (87%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 9 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for jobs.morpho.xyz (52.222.174.21)
Host is up (0.0055s latency).
Other addresses for jobs.morpho.xyz (not scanned):
2600:9000:218d:da00:1:bf30:e140:93a1 2600:9000:218d:2800:1:bf30:e140:93a1
2600:9000:218d:ba00:1:bf30:e140:93a1 2600:9000:218d:7c00:1:bf30:e140:93a1
2600:9000:218d:200:1:bf30:e140:93a1 2600:9000:218d:bc00:1:bf30:e140:93a1
```

Command

```
2600:9000:218d:c400:1:bf30:e140:93a1 2600:9000:218d:ce00:1:bf30:e140:93a1
52.222.174.100 52.222.174.101 52.222.174.52
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE  VERSION
80/tcp  open  http     Amazon CloudFront httpd
|_http-title: Did not follow redirect to https://jobs.morpho.xyz/
|_http-server-header: CloudFront
443/tcp open  ssl/http Amazon CloudFront httpd
| http-server-header:
|   AmazonS3
|_  CloudFront
|_http-title: Did not follow redirect to https://morpho-labs.notion.site/Morpho-
s-Open-Positions-e56ee0ec4e17438596ff7d573e5737e2/
| ssl-cert: Subject: commonName=jobs.morpho.xyz
| Subject Alternative Name: DNS:jobs.morpho.xyz, DNS:job.morpho.xyz
| Not valid before: 2023-02-24T00:00:00
|_Not valid after:  2023-09-06T23:59:59
Warning: OSScan results may be unreliable because we could not find at least 1
open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): FreeBSD 11.X|12.X (88%)
OS CPE: cpe:/o:freebsd:freebsd:11.1 cpe:/o:freebsd:freebsd:12.0
Aggressive OS guesses: FreeBSD 11.1-STABLE (88%), FreeBSD 12.0-RELEASE (88%),
FreeBSD 12.1-RELEASE (88%)
No exact OS matches for host (test conditions non-ideal).

Nmap scan report for telegram.morpho.xyz (18.164.52.53)
Host is up (0.017s latency).
Other addresses for telegram.morpho.xyz (not scanned):
2600:9000:2450:b600:1b:560f:5a40:93a1 2600:9000:2450:8c00:1b:560f:5a40:93a1
2600:9000:2450:ba00:1b:560f:5a40:93a1 2600:9000:2450:5e00:1b:560f:5a40:93a1
2600:9000:2450:f200:1b:560f:5a40:93a1 2600:9000:2450:8400:1b:560f:5a40:93a1
2600:9000:2450:f400:1b:560f:5a40:93a1 2600:9000:2450:3200:1b:560f:5a40:93a1
18.164.52.14 18.164.52.101 18.164.52.18
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE  VERSION
80/tcp  open  http     Amazon CloudFront httpd
|_http-server-header: CloudFront
|_http-title: Did not follow redirect to https://telegram.morpho.xyz/
443/tcp open  ssl/http Amazon CloudFront httpd
|_http-title: Did not follow redirect to https://t.me/MorphoDAO/
| http-server-header:
|   AmazonS3
|_  CloudFront
| ssl-cert: Subject: commonName=telegram.morpho.xyz
| Subject Alternative Name: DNS:telegram.morpho.xyz, DNS:tg.morpho.xyz
| Not valid before: 2023-02-22T00:00:00
|_Not valid after:  2023-09-06T23:59:59
Warning: OSScan results may be unreliable because we could not find at least 1
open and 1 closed port
Device type: phone|general purpose
Running (JUST GUESSING): Apple iOS 11.X|12.X|13.X (88%), Apple macOS
10.13.X|10.14.X|10.15.X (88%)
OS CPE: cpe:/o:apple:iphone_os:11 cpe:/o:apple:iphone_os:12
cpe:/o:apple:iphone_os:13 cpe:/o:apple:mac_os_x:10.13
cpe:/o:apple:mac_os_x:10.14 cpe:/o:apple:mac_os_x:10.15
Aggressive OS guesses: Apple macOS 10.13 (High Sierra) - 10.15 (Catalina) or iOS
11.0 - 13.4 (Darwin 17.0.0 - 19.2.0) (88%)
```

Command

```
No exact OS matches for host (test conditions non-ideal).

Nmap scan report for analytic.morpho.xyz (13.249.9.84)
Host is up (0.0064s latency).
Other addresses for analytic.morpho.xyz (not scanned):
2600:9000:2171:3c00:11:517d:e6c0:93a1 2600:9000:2171:de00:11:517d:e6c0:93a1
2600:9000:2171:c400:11:517d:e6c0:93a1 2600:9000:2171:5400:11:517d:e6c0:93a1
2600:9000:2171:2400:11:517d:e6c0:93a1 2600:9000:2171:8800:11:517d:e6c0:93a1
2600:9000:2171:a400:11:517d:e6c0:93a1 2600:9000:2171:7600:11:517d:e6c0:93a1
13.249.9.76 13.249.9.60 13.249.9.118
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE  VERSION
80/tcp  open  http     Amazon CloudFront httpd
|_http-server-header: CloudFront
|_http-title: Did not follow redirect to https://analytic.morpho.xyz/
443/tcp open  ssl/http Amazon CloudFront httpd
| ssl-cert: Subject: commonName=analytics.morpho.xyz
| Subject Alternative Name: DNS:analytics.morpho.xyz, DNS:analytic.morpho.xyz
| Not valid before: 2023-02-23T00:00:00
|_Not valid after:  2023-09-06T23:59:59
| http-server-header:
|   AmazonS3
|_  CloudFront
| http-title:  Analytics | Morpho
|_Requested resource was https://analytics.morpho.xyz/
Warning: OSScan results may be unreliable because we could not find at least 1
open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results
incomplete
No OS matches for host

Nmap scan report for graph.morpho.xyz (13.37.206.185)
Host is up (0.0062s latency).
Other addresses for graph.morpho.xyz (not scanned): 15.188.29.7 15.188.222.95
Not shown: 997 closed tcp ports (reset)
PORT    STATE    SERVICE   VERSION
25/tcp  filtered smtp
80/tcp  open     http      awselb/2.0
|_http-server-header: awselb/2.0
|_http-title: Did not follow redirect to https://graph.morpho.xyz:443/
| fingerprint-strings:
|   GetRequest, HTTPOptions:
|     HTTP/1.1 301 Moved Permanently
|     Server: awselb/2.0
|     Date: Wed, 03 May 2023 12:57:12 GMT
|     Content-Type: text/html
|     Content-Length: 134
|     Connection: close
|     Location: https://morpho-alb-274421675.eu-west-3.elb.amazonaws.com:443/
|     <html>
|     <head><title>301 Moved Permanently</title></head>
|     <body>
|     <center><h1>301 Moved Permanently</h1></center>
|     </body>
|     </html>
443/tcp open     ssl/https awselb/2.0
| fingerprint-strings:
|   FourOhFourRequest, GetRequest, HTTPOptions:
```

Command

```
|     HTTP/1.1 404 Not Found
|     Server: awselb/2.0
|     Date: Wed, 03 May 2023 12:57:18 GMT
|     Content-Type: text/plain; charset=utf-8
|     Content-Length: 16
|     Connection: close
|     found
| ssl-cert: Subject: commonName=graph.morpho.xyz
| Subject Alternative Name: DNS:graph.morpho.xyz
| Not valid before: 2023-03-13T00:00:00
|_Not valid after:  2024-04-10T23:59:59
| tls-alpn:
|   h2
|_  http/1.1
|_http-server-header: awselb/2.0
|_ssl-date: TLS randomness does not represent time
| tls-nextprotoneg:
|   h2
|_  http/1.1
|_http-title: Site doesn't have a title (text/plain; charset=utf-8).
Aggressive OS guesses: Linux 2.6.32 - 3.13 (93%), Linux 2.6.32 (90%), Linux 3.2
- 4.9 (90%), Linux 2.6.32 - 3.10 (90%), HP P2000 G3 NAS device (89%), Linux 5.4
(89%), Linux 2.6.32 - 3.1 (89%), Linux 3.7 (89%), Linux 2.4.18 (89%), Infomir
MAG-250 set-top box (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 15 hops

Nmap scan report for login.morpho.xyz (76.223.112.12)
Host is up (0.0063s latency).
Other addresses for login.morpho.xyz (not scanned): 13.248.245.245
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE  VERSION
80/tcp  open  http     Apache httpd
|_http-title: 421 Misdirected Request
|_http-server-header: Apache
443/tcp open  ssl/http Apache httpd
| ssl-cert: Subject: commonName=*.kerberos.okta.com/organizationName=Okta,
Inc./stateOrProvinceName=California/countryName=US
| Subject Alternative Name: DNS:*.kerberos.okta.com, DNS:kerberos.okta.com
| Not valid before: 2023-01-11T00:00:00
|_Not valid after:  2024-02-07T23:59:59
|_http-server-header: Apache
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|_  http/1.1
|_http-title: Okta - Page Not Found
Warning: OSScan results may be unreliable because we could not find at least 1
open and 1 closed port
Device type: phone
Running (JUST GUESSING): Google Android 5.X (90%)
OS CPE: cpe:/o:google:android:5.0.1
Aggressive OS guesses: Android 5.0.1 (90%)
No exact OS matches for host (test conditions non-ideal).

Nmap scan report for compound.morpho.xyz (13.32.145.54)
Host is up (0.0057s latency).
Other addresses for compound.morpho.xyz (not scanned): 13.32.145.104
13.32.145.47 13.32.145.46
```

Command

```
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE  VERSION
80/tcp  open  http     Amazon CloudFront httpd
|_http-title: Did not follow redirect to https://compound.morpho.xyz/
|_http-server-header: CloudFront
443/tcp open  ssl/http Amazon CloudFront httpd
| http-server-header:
|   AmazonS3
|_  CloudFront
|_http-title: Markets | Morpho
| ssl-cert: Subject: commonName=compound.morpho.xyz
| Subject Alternative Name: DNS:compound.morpho.xyz, DNS:staging.morpho.xyz
| Not valid before: 2023-02-24T00:00:00
|_Not valid after:  2023-06-25T23:59:59
Warning: OSScan results may be unreliable because we could not find at least 1
open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): FreeBSD 11.X (88%)
OS CPE: cpe:/o:freebsd:freebsd:11.1
Aggressive OS guesses: FreeBSD 11.1-RELEASE (88%), FreeBSD 11.1-STABLE (88%),
FreeBSD 11.0-RELEASE (86%), FreeBSD 11.0-STABLE (86%)
No exact OS matches for host (test conditions non-ideal).

Nmap scan report for analytics.morpho.xyz (13.32.145.40)
Host is up (0.015s latency).
Other addresses for analytics.morpho.xyz (not scanned):
2600:9000:20e1:6e00:8:c955:2c00:93a1 2600:9000:20e1:e00:8:c955:2c00:93a1
2600:9000:20e1:9e00:8:c955:2c00:93a1 2600:9000:20e1:a600:8:c955:2c00:93a1
2600:9000:20e1:c800:8:c955:2c00:93a1 2600:9000:20e1:f800:8:c955:2c00:93a1
2600:9000:20e1:9a00:8:c955:2c00:93a1 2600:9000:20e1:9000:8:c955:2c00:93a1
13.32.145.48 13.32.145.14 13.32.145.24
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE  VERSION
80/tcp  open  http     Amazon CloudFront httpd
|_http-server-header: CloudFront
|_http-title: Did not follow redirect to https://analytics.morpho.xyz/
443/tcp open  ssl/http Amazon CloudFront httpd
| http-server-header:
|   AmazonS3
|_  CloudFront
| ssl-cert: Subject: commonName=analytics.morpho.xyz
| Subject Alternative Name: DNS:analytics.morpho.xyz, DNS:analytic.morpho.xyz
| Not valid before: 2023-02-23T00:00:00
|_Not valid after:  2023-09-06T23:59:59
|_http-title:  Analytics | Morpho
Warning: OSScan results may be unreliable because we could not find at least 1
open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): FreeBSD 12.X|11.X (88%)
OS CPE: cpe:/o:freebsd:freebsd:12.0 cpe:/o:freebsd:freebsd:11.1
Aggressive OS guesses: FreeBSD 12.0-RELEASE (88%), FreeBSD 11.1-RELEASE (86%)
No exact OS matches for host (test conditions non-ideal).

Nmap scan report for vaults.morpho.xyz (13.32.145.21)
Host is up (0.0060s latency).
Other addresses for vaults.morpho.xyz (not scanned):
2600:9000:20e1:7800:1a:38f0:680:93a1 2600:9000:20e1:0:1a:38f0:680:93a1
2600:9000:20e1:a00:1a:38f0:680:93a1 2600:9000:20e1:9200:1a:38f0:680:93a1
```

Command

```
2600:9000:20e1:4e00:1a:38f0:680:93a1 2600:9000:20e1:cc00:1a:38f0:680:93a1
2600:9000:20e1:c200:1a:38f0:680:93a1 2600:9000:20e1:5e00:1a:38f0:680:93a1
13.32.145.60 13.32.145.81 13.32.145.111
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE  VERSION
80/tcp  open  http     Amazon CloudFront httpd
|_http-title: Did not follow redirect to https://vaults.morpho.xyz/
|_http-server-header: CloudFront
443/tcp open  ssl/http Amazon CloudFront httpd
|_http-title:  Vaults | Morpho
| http-server-header:
|   AmazonS3
|_  CloudFront
| ssl-cert: Subject: commonName=vaults.morpho.xyz
| Subject Alternative Name: DNS:vaults.morpho.xyz
| Not valid before: 2023-02-02T00:00:00
|_Not valid after:  2024-03-02T23:59:59
Warning: OSScan results may be unreliable because we could not find at least 1
open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): FreeBSD 11.X|12.X (88%)
OS CPE: cpe:/o:freebsd:freebsd:11.1 cpe:/o:freebsd:freebsd:12.0
Aggressive OS guesses: FreeBSD 11.1-STABLE (88%), FreeBSD 12.0-RELEASE (88%),
FreeBSD 12.1-RELEASE (88%)
No exact OS matches for host (test conditions non-ideal).

Nmap scan report for tg.morpho.xyz (18.164.52.101)
Host is up (0.0059s latency).
Other addresses for tg.morpho.xyz (not scanned):
2600:9000:2450:f400:1b:560f:5a40:93a1 2600:9000:2450:3200:1b:560f:5a40:93a1
2600:9000:2450:b600:1b:560f:5a40:93a1 2600:9000:2450:8c00:1b:560f:5a40:93a1
2600:9000:2450:ba00:1b:560f:5a40:93a1 2600:9000:2450:5e00:1b:560f:5a40:93a1
2600:9000:2450:f200:1b:560f:5a40:93a1 2600:9000:2450:8400:1b:560f:5a40:93a1
18.164.52.18 18.164.52.53 18.164.52.14
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE  VERSION
80/tcp  open  http     Amazon CloudFront httpd
|_http-title: Did not follow redirect to https://tg.morpho.xyz/
|_http-server-header: CloudFront
443/tcp open  ssl/http Amazon CloudFront httpd
| http-server-header:
|   AmazonS3
|_  CloudFront
|_http-title: Did not follow redirect to https://t.me/MorphoDAO/
| ssl-cert: Subject: commonName=telegram.morpho.xyz
| Subject Alternative Name: DNS:telegram.morpho.xyz, DNS:tg.morpho.xyz
| Not valid before: 2023-02-22T00:00:00
|_Not valid after:  2023-09-06T23:59:59
Warning: OSScan results may be unreliable because we could not find at least 1
open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): FreeBSD 11.X (88%)
OS CPE: cpe:/o:freebsd:freebsd:11.0
Aggressive OS guesses: FreeBSD 11.0-RELEASE (88%), FreeBSD 11.0-STABLE (88%),
FreeBSD 11.1-RELEASE (88%), FreeBSD 11.1-STABLE (88%)
No exact OS matches for host (test conditions non-ideal).

Nmap scan report for discord.morpho.xyz (143.204.231.87)
```

Command

```
Host is up (0.0068s latency).
Other addresses for discord.morpho.xyz (not scanned):
2600:9000:2113:ca00:1b:bc45:fac0:93a1 2600:9000:2113:7600:1b:bc45:fac0:93a1
2600:9000:2113:4600:1b:bc45:fac0:93a1 2600:9000:2113:1e00:1b:bc45:fac0:93a1
2600:9000:2113:c000:1b:bc45:fac0:93a1 2600:9000:2113:e800:1b:bc45:fac0:93a1
2600:9000:2113:e00:1b:bc45:fac0:93a1 2600:9000:2113:a600:1b:bc45:fac0:93a1
143.204.231.75 143.204.231.76 143.204.231.3
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE  VERSION
80/tcp  open  http     Amazon CloudFront httpd
|_http-server-header: CloudFront
|_http-title: Did not follow redirect to https://discord.morpho.xyz/
443/tcp open  ssl/http Amazon CloudFront httpd
|_http-title: Did not follow redirect to https://discord.com/invite/BWXbJMHMdz/
| http-server-header:
|   AmazonS3
|_  CloudFront
| ssl-cert: Subject: commonName=discord.morpho.xyz
| Subject Alternative Name: DNS:discord.morpho.xyz
| Not valid before: 2023-02-23T00:00:00
|_Not valid after:  2023-09-06T23:59:59
Warning: OSScan results may be unreliable because we could not find at least 1
open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): FreeBSD 11.X (88%)
OS CPE: cpe:/o:freebsd:freebsd:11.0
Aggressive OS guesses: FreeBSD 11.0-RELEASE (88%), FreeBSD 11.1-RELEASE (88%),
FreeBSD 11.1-STABLE (88%), FreeBSD 11.0-STABLE (86%)
No exact OS matches for host (test conditions non-ideal).

Nmap scan report for api.morpho.xyz (15.188.29.7)
Host is up (0.0053s latency).
Other addresses for api.morpho.xyz (not scanned): 15.188.222.95 13.37.206.185
Not shown: 997 closed tcp ports (reset)
PORT    STATE    SERVICE   VERSION
25/tcp  filtered smtp
80/tcp  open     http      awselb/2.0
|_http-server-header: awselb/2.0
|_http-title: Did not follow redirect to https://api.morpho.xyz:443/
| fingerprint-strings:
|   GetRequest, HTTPOptions:
|     HTTP/1.1 301 Moved Permanently
|     Server: awselb/2.0
|     Date: Wed, 03 May 2023 12:59:42 GMT
|     Content-Type: text/html
|     Content-Length: 134
|     Connection: close
|     Location: https://morpho-alb-274421675.eu-west-3.elb.amazonaws.com:443/
|     <html>
|     <head><title>301 Moved Permanently</title></head>
|     <body>
|     <center><h1>301 Moved Permanently</h1></center>
|     </body>
|     </html>
443/tcp open     ssl/https awselb/2.0
|_http-server-header: awselb/2.0
| tls-alpn:
|   h2
```

Command

```
|_  http/1.1
|_ssl-date: TLS randomness does not represent time
| tls-nextprotoneg:
|   h2
|_  http/1.1
|_http-cors: HEAD GET POST PUT DELETE PATCH
| ssl-cert: Subject: commonName=api.morpho.xyz
| Subject Alternative Name: DNS:api.morpho.xyz
| Not valid before: 2023-03-13T00:00:00
|_Not valid after:  2024-04-10T23:59:59
|_http-title: Swagger UI
| fingerprint-strings:
|   FourOhFourRequest, GetRequest, HTTPOptions:
|     HTTP/1.1 404 Not Found
|     Server: awselb/2.0
|     Date: Wed, 03 May 2023 12:59:48 GMT
|     Content-Type: text/plain; charset=utf-8
|     Content-Length: 16
|     Connection: close
|     found
Aggressive OS guesses: Linux 2.6.32 - 3.13 (93%), Linux 2.6.32 (90%), Linux 3.2
- 4.9 (90%), Linux 2.6.32 - 3.10 (90%), HP P2000 G3 NAS device (89%), Ubiquiti
AirMax NanoStation WAP (Linux 2.6.32) (89%), Linux 5.1 (89%), Linux 5.0 - 5.4
(89%), Ubiquiti Pico Station WAP (AirOS 5.2.6) (89%), Linux 2.6.32 - 3.1 (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 14 hops

Nmap scan report for integration.morpho.xyz (104.18.3.117)
Host is up (0.0048s latency).
Other addresses for integration.morpho.xyz (not scanned): 2606:4700::6812:375
2606:4700::6812:275 104.18.2.117
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE  VERSION
80/tcp   open  http     Cloudflare http proxy
|_http-server-header: cloudflare
|_http-title: Did not follow redirect to https://integration.morpho.xyz/
443/tcp  open  ssl/http Cloudflare http proxy
|_http-server-header: cloudflare
| ssl-cert: Subject: commonName=integration.morpho.xyz
| Subject Alternative Name: DNS:integration.morpho.xyz
| Not valid before: 2023-04-21T20:14:21
|_Not valid after:  2023-07-20T20:14:20
|_http-title: Welcome - Morpho Integrations Guides
8080/tcp open  http     Cloudflare http proxy
|_http-title: Did not follow redirect to https://integration.morpho.xyz:8080/
|_http-server-header: cloudflare
8443/tcp open  ssl/http Cloudflare http proxy
| ssl-cert: Subject: commonName=integration.morpho.xyz
| Subject Alternative Name: DNS:integration.morpho.xyz
| Not valid before: 2023-04-21T20:14:21
|_Not valid after:  2023-07-20T20:14:20
|_http-server-header: cloudflare
|_http-title: Welcome - Morpho Integrations Guides
Warning: OSScan results may be unreliable because we could not find at least 1
open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Linux 5.X|4.X (87%), FreeBSD 11.X (86%), OpenBSD 4.X
(85%)
```

Command

```
OS CPE: cpe:/o:linux:linux_kernel:5 cpe:/o:linux:linux_kernel:4.10
cpe:/o:freebsd:freebsd:11.0 cpe:/o:openbsd:openbsd:4.3
Aggressive OS guesses: Linux 5.0 - 5.4 (87%), Linux 4.10 (87%), FreeBSD 11.0-
RELEASE (86%), FreeBSD 11.0-STABLE (86%), FreeBSD 11.1-STABLE (86%), OpenBSD 4.3
(85%), FreeBSD 11.1-RELEASE (85%)
No exact OS matches for host (test conditions non-ideal).

Nmap scan report for admin.morpho.xyz (15.188.29.7)
Host is up (0.0051s latency).
Other addresses for admin.morpho.xyz (not scanned): 15.188.222.95 13.37.206.185
Not shown: 997 closed tcp ports (reset)
PORT    STATE    SERVICE   VERSION
25/tcp  filtered smtp
80/tcp  open     http      awselb/2.0
| fingerprint-strings:
|   FourOhFourRequest:
|   GetRequest, HTTPOptions:
|     HTTP/1.1 301 Moved Permanently
|     Server: awselb/2.0
|     Date: Wed, 03 May 2023 13:00:13 GMT
|     Content-Type: text/html
|     Content-Length: 134
|     Connection: close
|     Location: https://morpho-alb-274421675.eu-west-3.elb.amazonaws.com:443/
|     <html>
|     <head><title>301 Moved Permanently</title></head>
|     <body>
|     <center><h1>301 Moved Permanently</h1></center>
|     </body>
|     </html>
|_http-title: Did not follow redirect to https://admin.morpho.xyz:443/
|_http-server-header: awselb/2.0
443/tcp open     ssl/https awselb/2.0
|_http-server-header: awselb/2.0
| tls-nextprotoneg:
|   h2
|_  http/1.1
| tls-alpn:
|   h2
|_  http/1.1
|_ssl-date: TLS randomness does not represent time
|_http-title: Site doesn't have a title (text/plain; charset=utf-8).
| fingerprint-strings:
|   FourOhFourRequest, GetRequest, HTTPOptions:
|     HTTP/1.1 404 Not Found
|     Server: awselb/2.0
|     Date: Wed, 03 May 2023 13:00:19 GMT
|     Content-Type: text/plain; charset=utf-8
|     Content-Length: 16
|     Connection: close
|     found
| ssl-cert: Subject: commonName=admin.morpho.xyz
| Subject Alternative Name: DNS:admin.morpho.xyz
| Not valid before: 2023-03-13T00:00:00
|_Not valid after:  2024-04-10T23:59:59
Aggressive OS guesses: Linux 2.6.32 - 3.13 (93%), Linux 2.6.32 (90%), Linux 3.2
- 4.9 (90%), Linux 2.6.32 - 3.10 (90%), HP P2000 G3 NAS device (89%), Infomir
MAG-250 set-top box (89%), Ubiquiti AirMax NanoStation WAP (Linux 2.6.32) (89%),
```

Command

```
Linux 5.1 (89%), Linux 5.0 - 5.4 (89%), Ubiquiti Pico Station WAP (AirOS 5.2.6)
(89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 15 hops

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 31 IP addresses (31 hosts up) scanned in 258.30 seconds
```

Apart from the necessary open ports 80/443 used to deliver the web services, the scanner detected multiple open ports on the following hosts:

- integration.morpho.xyz (8080, 8443)
- vote.morpho.xyz (21 open HTTP ports)
- docs.morpho.xyz (8080, 8443)

Extending the attack surface increases the risk of security issues. It is advised to only open the necessary web services (80 and 443) and restrict/filter the other services.

Reverse proxy

A reverse proxy provided by Cloudflare seems to protect the web servers and the applications. This is a good security practice.

Web Application Firewall (WAF)

Command

```
$ wafw00f https://www.morpho.xyz
```

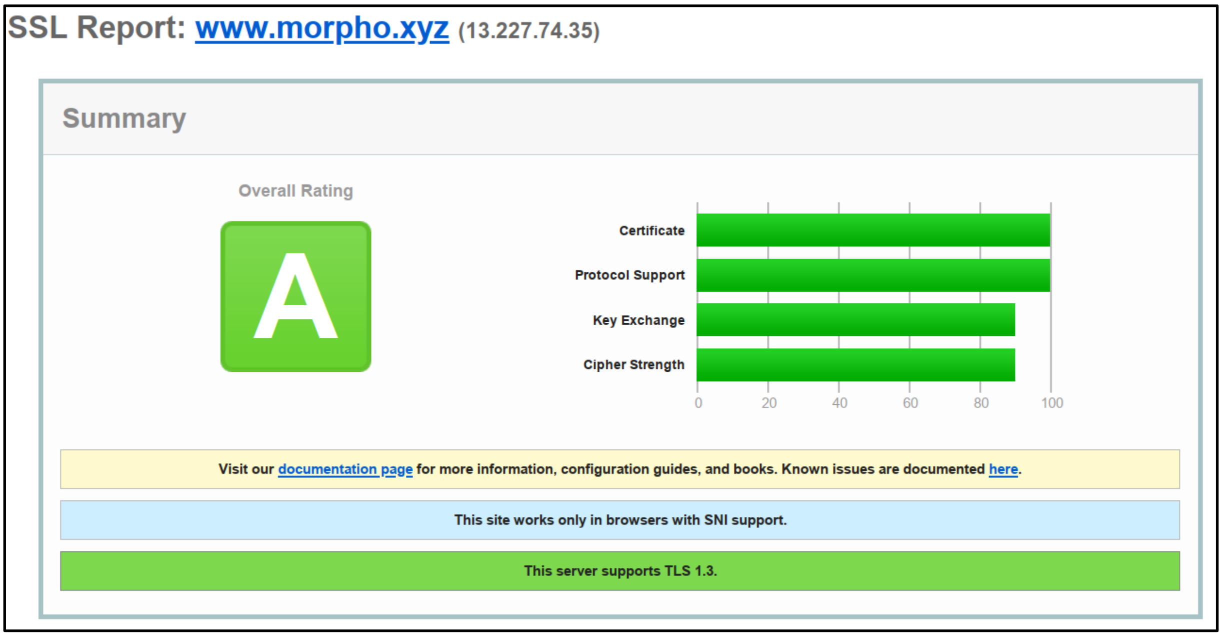
Output

```
[*] Checking https://www.morpho.xyz
[+] The site https://www.morpho.xyz is behind Cloudfront (Amazon) WAF.
[~] Number of requests: 2
```

The CloudFront Web Application Firewall (WAF) was detected.

SSL/TLS protocol management

No major weakness was identified on the audited server.



SSL Report: www.morpho.xyz (13.227.74.35)

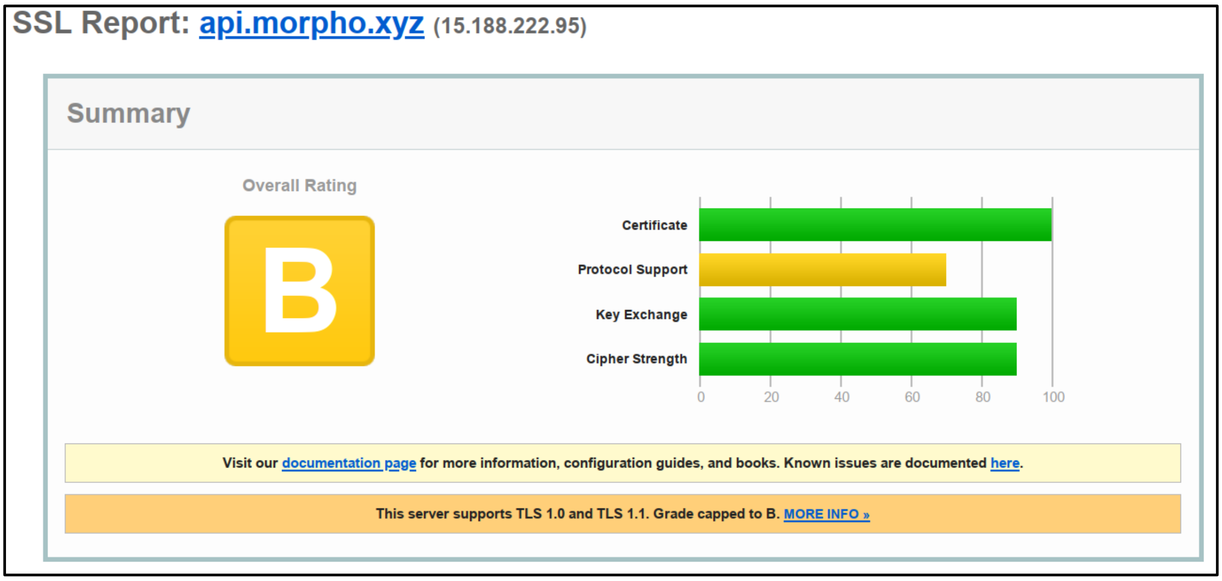
Summary

Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This site works only in browsers with SNI support.

This server supports TLS 1.3.

Figure 1: SSL configuration summary of www.morpho.xyz



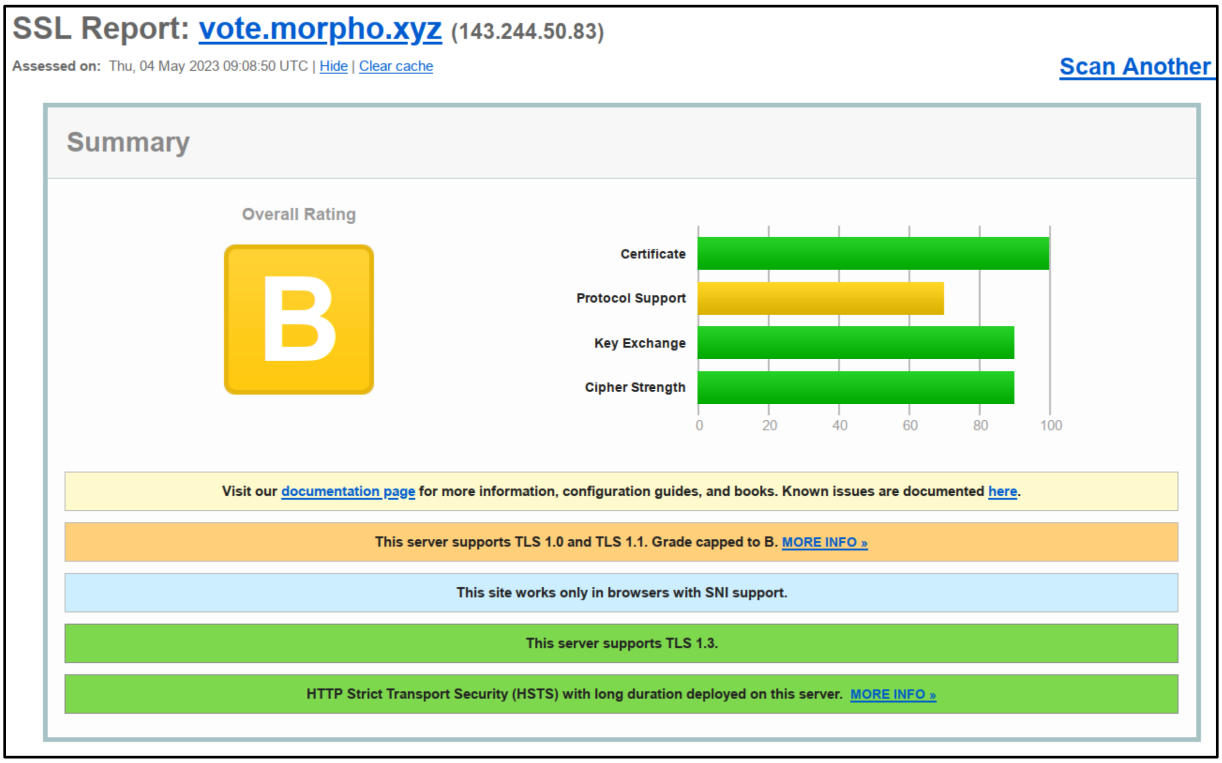
SSL Report: api.morpho.xyz (15.188.222.95)

Summary

Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This server supports TLS 1.0 and TLS 1.1. Grade capped to B. MORE INFO »

Figure 2: SSL configuration summary of api.morpho.xyz



SSL Report: vote.morpho.xyz (143.244.50.83)

Assessed on: Thu, 04 May 2023 09:08:50 UTC | Hide | Clear cache

Scan Another

Summary

Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This server supports TLS 1.0 and TLS 1.1. Grade capped to B. MORE INFO »

This site works only in browsers with SNI support.

This server supports TLS 1.3.

HTTP Strict Transport Security (HSTS) with long duration deployed on this server. MORE INFO »

Figure 3: SSL configuration summary of vote.morpho.xyz

However, the security could be improved by deactivating the support of the TLS protocols 1.0 and 1.1 on the following hosts:

- api.morpho.xyz
- vote.morpho.xyz
- ipfs.morpho.xyz
- admin.morpho.xyz
- graph.morpho.xyz

6 Audit results

After analysis of the public projects of the GitHub organizations linked to Morpho, **no sensitive data** was found in the source code.

CORS misconfiguration have been found, but no exploitation could be demonstrated in the audit time. Nevertheless, LEXFO recommends that the following principles be followed[5]:

→ Proper configuration of cross-origin requests

- If a web resource contains sensitive information, the origin should be properly specified in the Access-Control-Allow-Origin header.

→ Only allow trusted sites

- It may seem obvious but origins specified in the Access-Control-Allow-Origin header should only be sites that are trusted. In particular, dynamically reflecting origins from cross-origin requests without validation is readily exploitable and should be avoided.

→ Avoid whitelisting null

- Avoid using the header Access-Control-Allow-Origin: null. Cross-origin resource calls from internal documents and sandboxed requests can specify the null origin. CORS headers should be properly defined in respect of trusted origins for private and public servers.

→ Avoid wildcards in internal networks

- Avoid using wildcards in internal networks. Trusting network configuration alone to protect internal resources is not sufficient when internal browsers can access untrusted external domains.

→ CORS is not a substitute for server-side security policies

- CORS defines browser behaviors and is never a replacement for server-side protection of sensitive data - an attacker can directly forge a request from any trusted origin. Therefore, web servers should continue to apply protections over sensitive data, such as authentication and session management, in addition to properly configured CORS.

[5] https://portswigger.net/web-security/cors

6.1 V1: Exposed API keys

<table>
<tr><td>V1</td><td>Exposed API keys</td><td>STATUS
Proven</td><td>RISK
Low</td></tr>
<tr><td colspan="4">CONSEQUENCES
An attacker could steal the API key and use it in a way that would be unintended.</td></tr>
<tr><td colspan="4">AFFECTED COMPONENTS
– https://aave.morpho.xyz
– https://vaults.morpho.xyz
– https://governance.morpho.xyz
– https://compound.morpho.xyz
– https://app.morpho.xyz</td></tr>
<tr><td colspan="4">MITIGATION
Authenticate requests to the Infura API.</td></tr>
<tr><td colspan="2">EXPLOITABILITY
Difficult</td><td>IMPACT
Insignificant</td><td>CORRECTION DIFFICULTY
Simple</td></tr>
</table>

Affected components

Source code:

→ morpho-offchain-main/dapps/*/config/index.ts

Websites:

→ https://aave.morpho.xyz
→ https://vaults.morpho.xyz
→ https://governance.morpho.xyz
→ https://compound.morpho.xyz
→ https://app.morpho.xyz

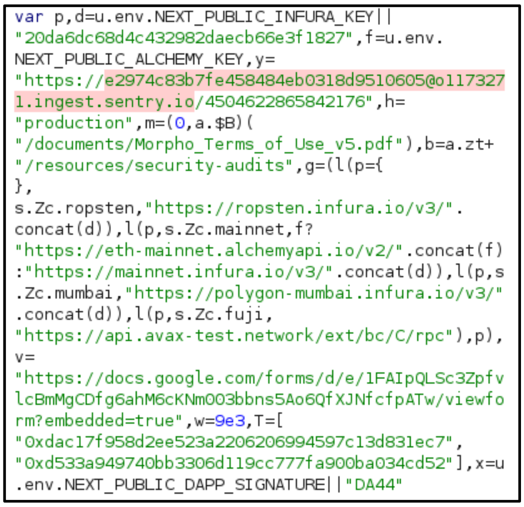
Prerequisites

→ None

Description

Several dApps deployed on the following hosts expose API keys in their client-side JavaScript bundle:

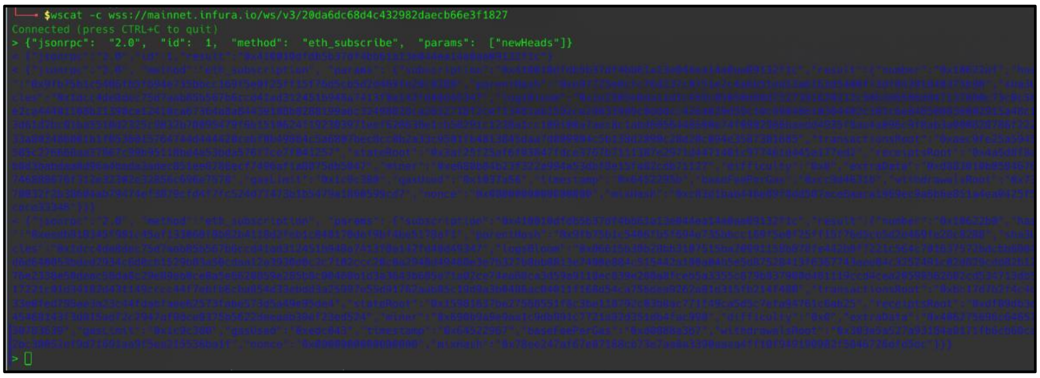
- aave.morpho.xyz
- vaults.morpho.xyz
- governance.morpho.xyz
- compound.morpho.xyz
- app.morpho.xyz



```
var p,d=u.env.NEXT_PUBLIC_INFURA_KEY||
"20da6dc68d4c432982daecb66e3f1827",f=u.env.
NEXT_PUBLIC_ALCHEMY_KEY,y=
"https://e2974c83b7fe458484eb0318d9510605@o117327
1.ingest.sentry.io/4504622865842176",h=
"production",m=(0,a.$B)(
"/documents/Morpho_Terms_of_Use_v5.pdf"),b=a.zt+
"/resources/security-audits",g=(l(p={
},
s.Zc.ropsten,"https://ropsten.infura.io/v3/".
concat(d)),l(p,s.Zc.mainnet,f?
"https://eth-mainnet.alchemyapi.io/v2/".concat(f)
:"https://mainnet.infura.io/v3/".concat(d)),l(p,s
.Zc.mumbai,"https://polygon-mumbai.infura.io/v3/"
.concat(d)),l(p,s.Zc.fuji,
"https://api.avax-test.network/ext/bc/C/rpc"),p),
v=
"https://docs.google.com/forms/d/e/1FAIpQLSc3Zpfv
lcBmMgCDfg6ahM6cKNm003bbns5Ao6QfXJNfcfpATw/viewfo
rm?embedded=true",w=9e3,T=[
"0xdac17f958d2ee523a2206206994597c13d831ec7",
"0xd533a949740bb3306d119cc777fa900ba034cd52"],x=u
.env.NEXT_PUBLIC_DAPP_SIGNATURE||"DA44"
```

Figure 4: Application configuration available client-side

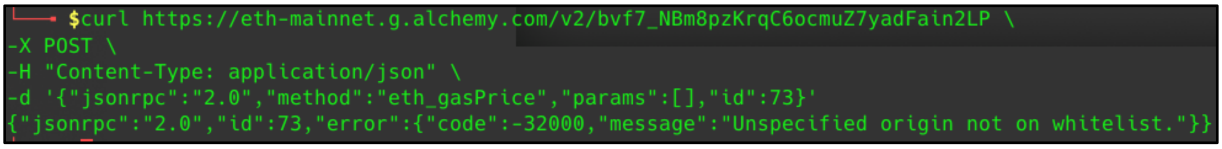
An attacker can use the provided Infura API key to subscribe to events, for instance fires a notification each time a new header is appended to the chain:



```
└──╼ $wscat -c wss://mainnet.infura.io/ws/v3/20da6dc68d4c432982daecb66e3f1827
Connected (press CTRL+C to quit)
> {"jsonrpc":  "2.0",  "id":  1,  "method":  "eth_subscribe",  "params":  ["newHeads"]}
[illegible]
> 
```

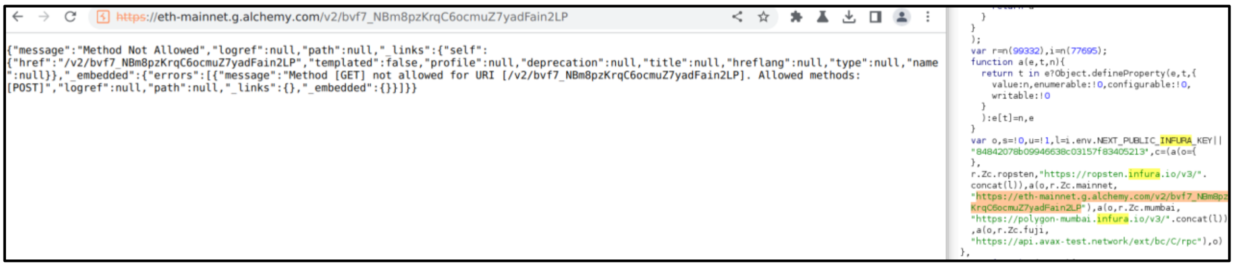
Figure 5: Infura event subscription

The exposed Alchemy API key is protected by a whitelist and cannot be exploited by an attacker.



```
└──╼ $curl https://eth-mainnet.g.alchemy.com/v2/bvf7_NBm8pzKrqC6ocmuZ7yadFain2LP \
-X POST \
-H "Content-Type: application/json" \
-d '{"jsonrpc":"2.0","method":"eth_gasPrice","params":[],"id":73}'
{"jsonrpc":"2.0","id":73,"error":{"code":-32000,"message":"Unspecified origin not on whitelist."}}
```

Figure 6: Whitelist protection of the Alchemy API key



https://eth-mainnet.g.alchemy.com/v2/bvf7_NBm8pzKrqC6ocmuZ7yadFain2LP

```
{"message":"Method Not Allowed","logref":null,"path":null,"_links":{"self":
{"href":"/v2/bvf7_NBm8pzKrqC6ocmuZ7yadFain2LP","templated":false,"profile":null,"deprecation":null,"title":null,"hreflang":null,"type":null,"name
":null}},"_embedded":{"errors":[{"message":"Method [GET] not allowed for URI [/v2/bvf7_NBm8pzKrqC6ocmuZ7yadFain2LP]. Allowed methods:
[POST]","logref":null,"path":null,"_links":{},"_embedded":{}}]}}
```

```
      }
    }
    );
    var r=n(99332),i=n(77695);
    function a(e,t,n){
      return t in e?Object.defineProperty(e,t,{
        value:n,enumerable:!0,configurable:!0,
        writable:!0
      }
      ):e[t]=n,e
    }
    var o,s=!0,u=!1,l=i.env.NEXT_PUBLIC_INFURA_KEY||
    "84842078b09946638c03157f83405213",c=(a(o={
    },
    r.Zc.ropsten,"https://ropsten.infura.io/v3/".
    concat(l)),a(o,r.Zc.mainnet,
    "https://eth-mainnet.g.alchemy.com/v2/bvf7_NBm8pz
    KrqC6ocmuZ7yadFain2LP"),a(o,r.Zc.mumbai,
    "https://polygon-mumbai.infura.io/v3/".concat(l))
    ,a(o,r.Zc.fuji,
    "https://api.avax-test.network/ext/bc/C/rpc"),o)
  },
```

Figure 7: Second occurrence of exposed API keys in client code

Impact

The Infura and Alchemy API keys are considered to be non-sensitive API keys. However, these service providers have various rate-limiting on the requests and an attacker could steal the API key and use it in a way that would be unintended.

Mitigation

To fix this vulnerability, LEXFO recommends removing the API keys from the JavaScript code when possible. It is commonly recommended to use the secret management functionality of the cloud provider (AWS secrets) or to use environment variables.

For securing API keys in client-side only applications, see for instance Securing keys in frontend only dApps.

Lexfo recommends referring to the documentation of the API publisher for securing the API keys:

- → Infura: authenticate all requests with a project secret or JWT, use allowlists.
- → Alchemy: set up an allowlist within your Alchemy dashboard, specifying what domains, contract addresses, wallet addresses, or IP addresses are able to send requests.

6.2 V2: Default configuration of CloudTrail log

V2	Default configuration of CloudTrail log	STATUS Proven	RISK Medium
CONSEQUENCES An attacker with access to the CloudTrail log could identify a weakness in the use or configuration of an account.			
AFFECTED COMPONENTS CloudTrail: – management-events			
MITIGATION To fix this vulnerability, it is recommended to harden the configuration: validate the log file, encrypt the trails with the KMS key and attach a CloudWatch Logs group. → Set log file validation to: Yes → Ensure that the Trail is encrypted with the KMS key			
EXPLOITABILITY Moderate	IMPACT Limited	CORRECTION DIFFICULTY Simple	

Affected components

→ CloudTrail : management-events

Prerequisites

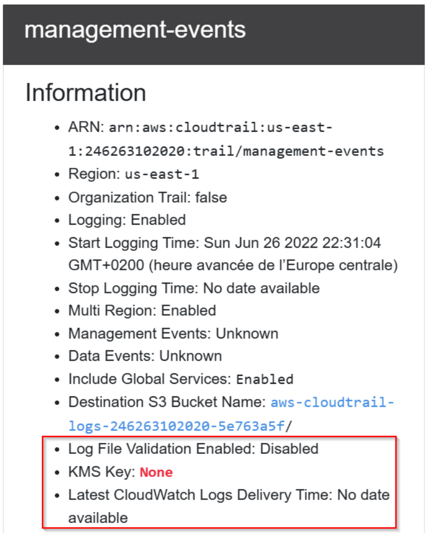
→ None

Description

AWS CloudTrail is a web service that records AWS API calls for your account and delivers log files to you. The recorded information includes the identity of the API caller, the time of the API call, the source IP address of the API caller, the request parameters, and the response elements returned by the AWS service. CloudTrail provides a history of AWS API calls for an account, including API calls made via the Management Console, SDKs, command line tools, and higher-level AWS services (such as CloudFormation).

A trail named "management-events has different configuration defaults:

→ Log File Validation Enabled: log file validation provides integrity on CloudTrail log files.
→ KMS Key : encryption with SSE-KMS provides confidentiality on CloudTrail log files.
→ Latest CloudWatch Logs Delivery Time: Trail integration with CloudWatch allows you to set up alarms and notifications on suspicious account behavior.



management-events

Information

- ARN: arn:aws:cloudtrail:us-east-1:246263102020:trail/management-events
- Region: us-east-1
- Organization Trail: false
- Logging: Enabled
- Start Logging Time: Sun Jun 26 2022 22:31:04 GMT+0200 (heure avancée de l'Europe centrale)
- Stop Logging Time: No date available
- Multi Region: Enabled
- Management Events: Unknown
- Data Events: Unknown
- Include Global Services: Enabled
- Destination S3 Bucket Name: aws-cloudtrail-logs-246263102020-5e763a5f/
- Log File Validation Enabled: Disabled
- KMS Key: None
- Latest CloudWatch Logs Delivery Time: No date available

Figure 8 - Configuration of Trail: management-events

Impact

Strengthening the CloudTrail log configuration provides efficient event tracking and confidentiality.

Mitigation

To fix this vulnerability, LEXFO recommends to:

- → Set log file validation to : Yes
- → Ensure that the Trail is encrypted with the KMS key
- → Configure the Trail to have a CloudWatch Logs group attached

6.3 V3: Weak password policy

<table>
<tr><td>V3</td><td>Weak password policy</td><td colspan="2">STATUS
Proven</td><td>RISK
Low</td></tr>
<tr><td colspan="5">CONSEQUENCES
An attacker can discover the passwords of users on the tenant. He can then easily authenticate himself without the user's knowledge and access sensitive information. However, the risk is reduced because all users are subject to multi-factor authentication.</td></tr>
<tr><td colspan="5">AFFECTED COMPONENTS
Amazon Web Service:
– IAM</td></tr>
<tr><td colspan="5">MITIGATION
→ Implement a strong password policy.
→ Apply specific rules according to the type of account (user, admin, service)</td></tr>
<tr><td>EXPLOITABILITY
Very difficult</td><td colspan="2">IMPACT
Limited</td><td colspan="2">CORRECTION DIFFICULTY
Simple</td></tr>
</table>

Affected components

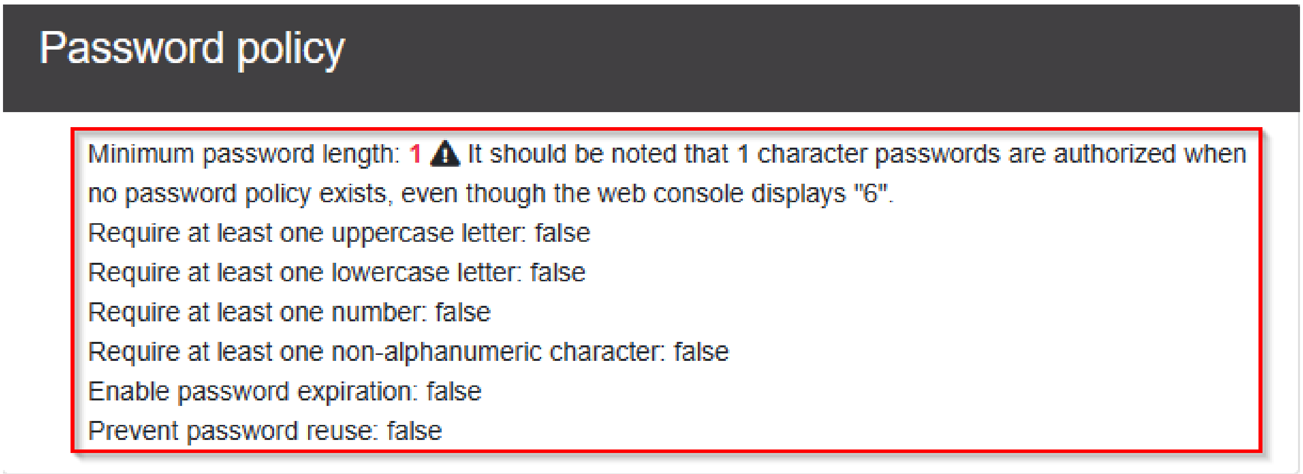
Amazon Web Service:

- → IAM

Prerequisites

- → None

Description



Password policy

Minimum password length: 1 ⚠ It should be noted that 1 character passwords are authorized when no password policy exists, even though the web console displays "6".
Require at least one uppercase letter: false
Require at least one lowercase letter: false
Require at least one number: false
Require at least one non-alphanumeric character: false
Enable password expiration: false
Prevent password reuse: false

Figure 2 – Weak password policy

Impact

An attacker can discover the passwords of users on the tenant. However, the risk is reduced because all users are subject to multifactor authentication.

Mitigation

To fix this vulnerability, LEXFO recommends:

- → Implement a strong password policy. For more information on the ANSSI recommendations, see: https://www.ssi.gouv.fr/guide/mot-de-passe/ . A strong password:
    - Must have a minimum length of 12 characters
    - Must contain at least one number and one letter
    - Must contain at least one upper and one lower case letter
    - Must contain at least one special character (non-alphanumeric)
- → Apply specific rules according to the type of account, for example:
    - Maximum password age for administrative accounts : 60 days
    - Maximum password age for service accounts : 365 days
    - Minimum length for administrative accounts : 16 characters
    - Minimum length for service accounts : 24 characters

6.4 V4: Root Account Used Recently

<table>
<tr><td>V4</td><td colspan="2">Root Account Used Recently</td><td>STATUS
Proven</td><td>RISK
Low</td></tr>
<tr><td colspan="5">CONSEQUENCES
The "root" user has unlimited access to and control of all account resources. Use of this account is inconsistent with the principles of least privilege and segregation of duties, and may result in unnecessary damage due to an account error or compromise.</td></tr>
<tr><td colspan="5">AFFECTED COMPONENTS
Amazon Web Service:
– IAM</td></tr>
<tr><td colspan="5">MITIGATION
Disable or delete all access keys associated with the "root" user.</td></tr>
<tr><td colspan="2">EXPLOITABILITY
Very difficult</td><td colspan="2">IMPACT
Limited</td><td>CORRECTION DIFFICULTY
Moderate</td></tr>
</table>

Affected components

Amazon Web Service:

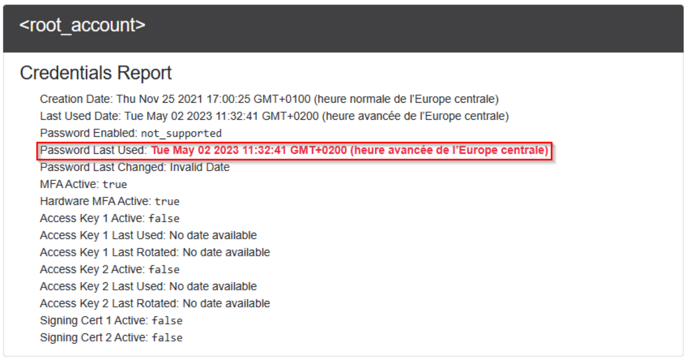
- → IAM

Prerequisites

- → None

Description

When an AWS account is created, a "root user" is created that cannot be disabled or deleted. This user has unlimited access and control over all resources in the AWS account. It is strongly recommended to avoid using this account for day-to-day tasks.



<root_account>

Credentials Report

Creation Date: Thu Nov 25 2021 17:00:25 GMT+0100 (heure normale de l'Europe centrale)
Last Used Date: Tue May 02 2023 11:32:41 GMT+0200 (heure avancée de l'Europe centrale)
Password Enabled: not_supported
Password Last Used: Tue May 02 2023 11:32:41 GMT+0200 (heure avancée de l'Europe centrale)
Password Last Changed: Invalid Date
MFA Active: true
Hardware MFA Active: true
Access Key 1 Active: false
Access Key 1 Last Used: No date available
Access Key 1 Last Rotated: No date available
Access Key 2 Active: false
Access Key 2 Last Used: No date available
Access Key 2 Last Rotated: No date available
Signing Cert 1 Active: false
Signing Cert 2 Active: false

Figure 2 – Root Account Used Recently

Impact

It is recommended to use other accounts for administration tasks.

Mitigation

To fix this vulnerability, LEXFO recommends to:

If you find that the "root" user account is being used for day-to-day activities, including administrative tasks that do not require the "root" user, do the following administrative tasks that do not require the "root" user:

1. Change the password for the "root" user.
2. Disable or delete all access keys associated with the "root" user.

6.5 V5: Obsolete AWS access key

V5	Obsolete AWS access key	STATUS Proven	RISK Low

CONSEQUENCES

The presence of obsolete access keys increases the attack surface and the risk of compromise.

AFFECTED COMPONENTS

Amazon Web Service:

- IAM

MITIGATION

- → Delete inactive AWS access keys
- → Force a rotation of AWS access keys every 90 days

EXPLOITABILITY Very difficult	IMPACT Limited	CORRECTION DIFFICULTY Moderate

Affected components

Amazon Web Service:

- → IAM

Prerequisites

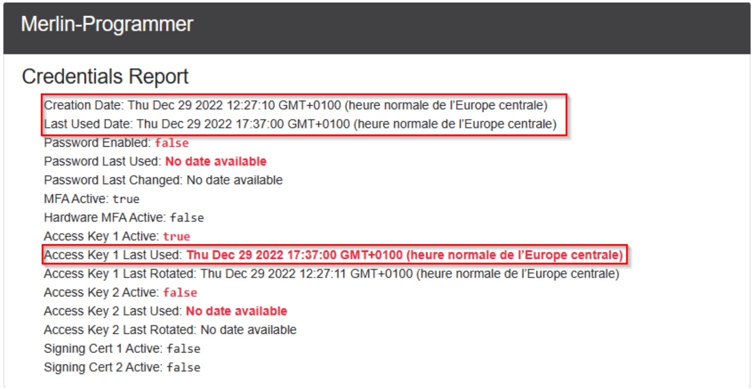
- → None

Description

AWS IAM users can access AWS resources using different types of credentials, such as passwords or access keys.

It is recommended to disable or delete obsolete service accounts:

- → Merlin-Programmer
- → Mathis-Programmer



Merlin-Programmer

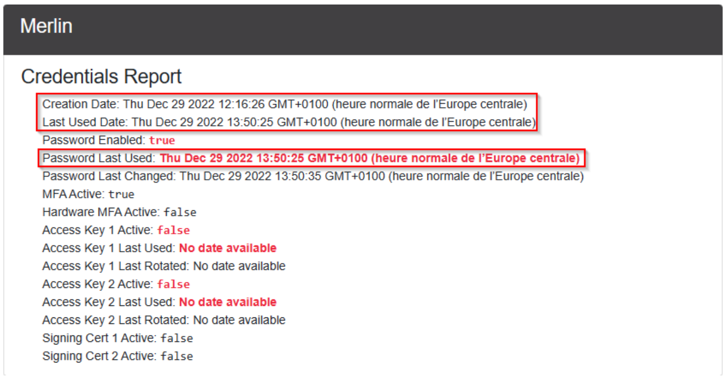
Credentials Report

```
Creation Date: Thu Dec 29 2022 12:27:10 GMT+0100 (heure normale de l'Europe centrale)
Last Used Date: Thu Dec 29 2022 17:37:00 GMT+0100 (heure normale de l'Europe centrale)
Password Enabled: false
Password Last Used: No date available
Password Last Changed: No date available
MFA Active: true
Hardware MFA Active: false
Access Key 1 Active: true
Access Key 1 Last Used: Thu Dec 29 2022 17:37:00 GMT+0100 (heure normale de l'Europe centrale)
Access Key 1 Last Rotated: Thu Dec 29 2022 12:27:11 GMT+0100 (heure normale de l'Europe centrale)
Access Key 2 Active: false
Access Key 2 Last Used: No date available
Access Key 2 Last Rotated: No date available
Signing Cert 1 Active: false
Signing Cert 2 Active: false
```

Figure 2 – Example of inactive service account

The audit identified 3 accounts which are not used regularly:

→ Mathis
→ Merlin
→ Julien



Merlin

Credentials Report

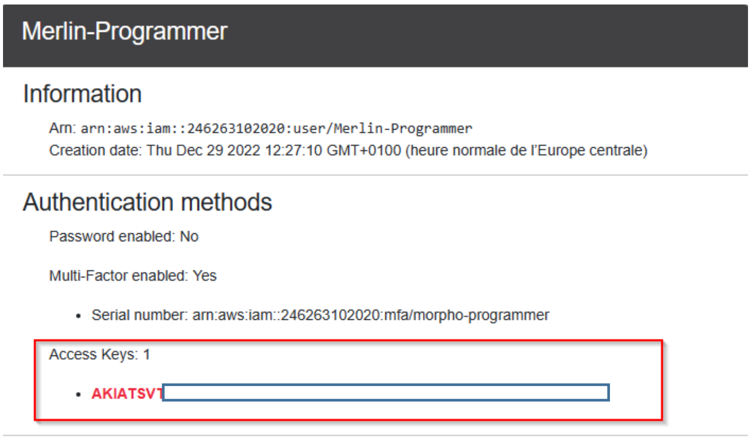
Creation Date: Thu Dec 29 2022 12:16:26 GMT+0100 (heure normale de l'Europe centrale)
Last Used Date: Thu Dec 29 2022 13:50:25 GMT+0100 (heure normale de l'Europe centrale)
Password Enabled: true
Password Last Used: Thu Dec 29 2022 13:50:25 GMT+0100 (heure normale de l'Europe centrale)
Password Last Changed: Thu Dec 29 2022 13:50:35 GMT+0100 (heure normale de l'Europe centrale)
MFA Active: true
Hardware MFA Active: false
Access Key 1 Active: false
Access Key 1 Last Used: No date available
Access Key 1 Last Rotated: No date available
Access Key 2 Active: false
Access Key 2 Last Used: No date available
Access Key 2 Last Rotated: No date available
Signing Cert 1 Active: false
Signing Cert 2 Active: false

Figure 9 – Example of inactive user account

It is recommended to ensure the password policy is applied for these accounts (**V4**), with a regular update of passwords if needed.

In addition, it is recommended that you enable the AWS access key rotation (active) feature at a frequency of 90 days. This will reduce the risk of having an obsolete key:

→ Merlin-Programmer
→ Mathis-Programmer
→ Julien-Neo



Merlin-Programmer

Information

Arn: arn:aws:iam::246263102020:user/Merlin-Programmer
Creation date: Thu Dec 29 2022 12:27:10 GMT+0100 (heure normale de l'Europe centrale)

Authentication methods

Password enabled: No

Multi-Factor enabled: Yes

- Serial number: arn:aws:iam::246263102020:mfa/morpho-programmer

Access Keys: 1

- AKIATSV[redacted]

Figure 10 – Inactive AWS access key

Impact

It is recommended to contact the owners of these accounts before their deletions.

Mitigation

To fix this vulnerability, LEXFO recommends to:

→ Delete inactive AWS access keys
→ Force a rotation of AWS access keys (active) every 90 days

6.6 V6: Misconfiguration of S3 Bucket

<table>
<tr><td>V6</td><td colspan="2">Misconfiguration of S3 Bucket</td><td>STATUS
Proven</td><td>RISK
Low</td></tr>
<tr><td colspan="5">CONSEQUENCES
Misconfiguration have been found on all the following AWS storage services Bucket S3.</td></tr>
<tr><td colspan="5">AFFECTED COMPONENTS
Amazon Web Service:
– Bucket S3</td></tr>
<tr><td colspan="5">MITIGATION
→ 1. Enable the MFA Delete feature
→ 2. Enable access logging
→ 3. Force HTTPS communication
→ 4. Enable versioning</td></tr>
<tr><td colspan="2">EXPLOITABILITY
Very difficult</td><td colspan="2">IMPACT
Limited</td><td>CORRECTION DIFFICULTY
Moderate</td></tr>
</table>

Affected components

Amazon Web Service:

- → IAM

Prerequisites

- → None

Description

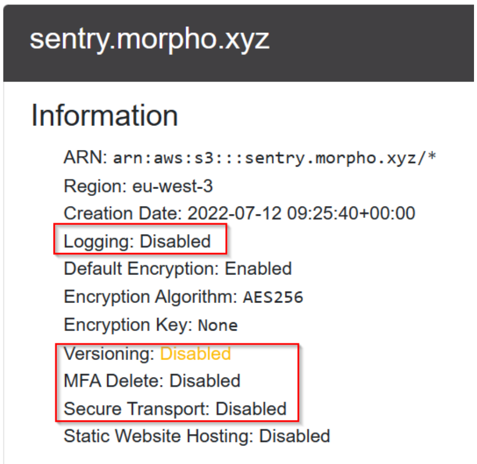
1. Enable MFA delete to help protect objects from accidental or unauthorized deletion. It should be noted that MFA Delete can only be configured on buckets that have versioning enabled.

2. Server access logging provides detailed records of the requests that are made to a bucket. Server access logs can assist you in security and access audits, help you learn about your customer base, and understand your Amazon S3 bill.

3. If HTTPS is not enforced on the bucket policy, communication between clients and S3 buckets can use unencrypted HTTP. As a result, sensitive information could be transmitted in clear text over the network|Internet.

4. Versioning is a means of keeping multiple variants of an object in the same bucket. With versioning, you can easily recover from both unintended user actions and application failures.

All 49 buckets are affected by these misconfigurations.



sentry.morpho.xyz

Information

ARN: arn:aws:s3:::sentry.morpho.xyz/*
Region: eu-west-3
Creation Date: 2022-07-12 09:25:40+00:00
Logging: Disabled
Default Encryption: Enabled
Encryption Algorithm: AES256
Encryption Key: None
Versioning: Disabled
MFA Delete: Disabled
Secure Transport: Disabled
Static Website Hosting: Disabled

Figure 2 – Misconfiguration of sentry.morpho.xyz Bucket

Impact

N/A

Mitigation

To fix this vulnerability, LEXFO recommends for all S3 buckets:

- → 1. Enable the MFA Delete feature
- → 2. Enable access logging
- → 3. Force HTTPS communication
- → 4. Enable versioning

6.7 V7: Misconfiguration of VPC

<table>
<tr><td>V7</td><td colspan="2">Misconfiguration of VPC</td><td>STATUS
Proven</td><td>RISK
Low</td></tr>
<tr><td colspan="5">CONSEQUENCES
Access to remote server administration ports, such as 22 and 3389, increases the attack surface of resources and unnecessarily increases the risk of resource compromise.</td></tr>
<tr><td colspan="5">AFFECTED COMPONENTS
Amazon Web Service:
– VPC</td></tr>
<tr><td colspan="5">MITIGATION
Harden VPC NACL rules and creating Flow Logs for event logging.</td></tr>
<tr><td colspan="2">EXPLOITABILITY
Difficult</td><td>IMPACT
Insignificant</td><td colspan="2">CORRECTION DIFFICULTY
Moderate</td></tr>
</table>

Affected components

Amazon Web Service:

→ VPC

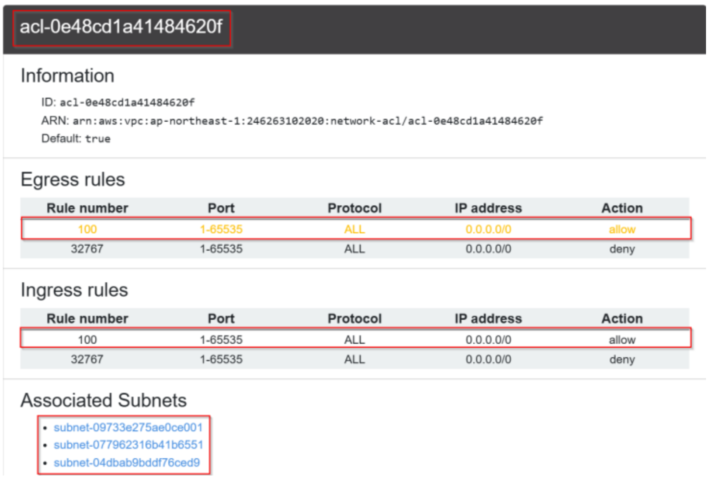
Prerequisites

→ None

Description

The Network Access Control List (NACL) function provide stateless filtering of ingress and egress network traffic to AWS resources. It is recommended that no NACL allows unrestricted ingress access to remote server administration ports, such as SSH to port 22 and RDP to port 3389.

All of these NACLs (17 NACLs) allow all Ingress and Egress traffic. In addition, all VPC subnets (55 Subnets) inherit these rules.



acl-0e48cd1a41484620f

Information

ID: acl-0e48cd1a41484620f
ARN: arn:aws:vpc:ap-northeast-1:246263102020:network-acl/acl-0e48cd1a41484620f
Default: true

Egress rules

Rule number	Port	Protocol	IP address	Action
100	1-65535	ALL	0.0.0.0/0	allow
32767	1-65535	ALL	0.0.0.0/0	deny

Ingress rules

Rule number	Port	Protocol	IP address	Action
100	1-65535	ALL	0.0.0.0/0	allow
32767	1-65535	ALL	0.0.0.0/0	deny

Associated Subnets

- subnet-09733e275ae0ce001
- subnet-077962316b41b6551
- subnet-04dbab9bddf76ced9

Figure 2 – Example of NACL with 3 associated subnets

In addition, the functionality Flow Logs is disabled on the 55 subnets. Flow logs enable the investigation of incidents involving unauthorized network traffic, such as an attacker exfiltrating data or pivoting to other hosts.

Impact

As the identified VPCs do not concern production components, and because of the good segregation the impact is low.

Mitigation

To fix this vulnerability, LEXFO recommends hardening VPC NACL rules and creating Flow Logs for event logging.

6.8 V8: AWS Config not enabled

V8	AWS Config not enabled	STATUS Proven	RISK Medium
CONSEQUENCES No AWS Config recorders are configured, which means that changes in AWS resource configuration are not logged. This hinders security analysis, resource change tracking and compliance auditing.			
AFFECTED COMPONENTS Amazon Web Service: – IAM			
MITIGATION Enable an AWS Config for all regions.			
EXPLOITABILITY Moderate	IMPACT Limited	CORRECTION DIFFICULTY Simple	

Affected components

Amazon Web Service:

Prerequisites

- → None

Description

AWS Config is a web service that performs configuration management of supported AWS resources within your account and delivers log files to you. The recorded information includes the configuration item (AWS resource), relationships between configuration items (AWS resources), any configuration changes between resources. It is recommended AWS Config be enabled in all regions.

Impact

It is recommended AWS Config be enabled in all regions.

Mitigation

To fix this vulnerability, LEXFO recommends to implement AWS Config configuration.

From Console:

- 1. Select the region you want to focus on in the top right of the console
- 2. Click Services
- 3. Click Config
- 4. Define which resources you want to record in the selected region
- 5. Choose to include global resources (IAM resources)
- 6. Specify an S3 bucket in the same account or in another managed AWS account

- 7. Create an SNS Topic from the same AWS account or another managed AWS account