# Surface Analysis and Network Penetration Test

# GLOBALEAKS External Perimeter

CONFIDENTIAL

V1.3 - January 2024

Public document, disclosure permitted on customer website.

# 1 Executive summary

ISGroup S.r.l has been hired by "Whistleblowing Solutions Impresa Sociale S.r.l." (project sponsor) to perform a Network Penetration Test activity on the "GLOBALEAKS" external perimeter.

Several administrative interfaces are exposed to the internet (3.1 Exposed Administrative Interface). An attacker can detect such interfaces and perform specific attacks, as Password Guessing or exploit a known vulnerability.

Some hosts are not protected against the Channels Downgrade Attacks (3.2 Strict Transport Security (HSTS) not enforced). A MiTM is possible.

Some TLS certificates are self-signed (3.3 SSL Self-Signed Certificate) and/or expired (3.4 SSL Certificate Expiry). A MiTM is possible.

Some hosts disclose their technology (3.5 Technology or Version Disclosure). An attacker can use this information to perform targeted attacks.

| Targets in scope | | |
|---|---|---|
| fs1.globaleaks.org | SERVER1 | 95.174.23.115 |
| fs2.globaleaks.org | SERVER2 | 95.174.28.200 |
| vc.globaleaks.org | VCENTER | 95.174.23.114 |
| fw1.globaleaks.org | FIREWALL (PRIMARY) | 37.9.228.30 |
| fw2.globaleaks.org | FIREWALL (SECONDARY) | 37.9.228.59 |
| fw-carp.globaleaks.org | FIREWALL (CARP) | 37.9.228.20 |
| www.globaleaks.org | PUBLIC SITE | 95.174.23.119 |
| deb.globaleaks.org | SOFTWARE REPOSITORY | 95.174.23.119 |
| mail.globaleaks.org | MAIL SERVER | 95.174.23.113 |
| try.globaleaks.org | DEMO SERVER | 95.174.28.205 |

*Sincerely, the audit team*
*Francesco Ongaro, Pasquale Fiorillo and Marco Lunardi*

## 2 Technical summary

We recommend fixing found issues in the order suggested by this table.

| Vulnerability | | Impact |
|---|---|---|
| 3.1 | Exposed Administrative Interface | High |
| 3.2 | Strict Transport Security (HSTS) not enforced | Medium |
| 3.3 | SSL Self-Signed Certificate | Medium |
| 3.4 | SSL Certificate Expiry | Medium |
| 3.5 | Technology or Version Disclosure | Low |
| 3.6 | TLS Version 1.2 Protocol Detection | Info |
| 3.7 | TLS Version 1.3 Protocol Detection | Info |

# 3 Network Penetration Test

A network penetration test is a security exercise where a cybersecurity expert attempts to find and exploit vulnerabilities in a network.

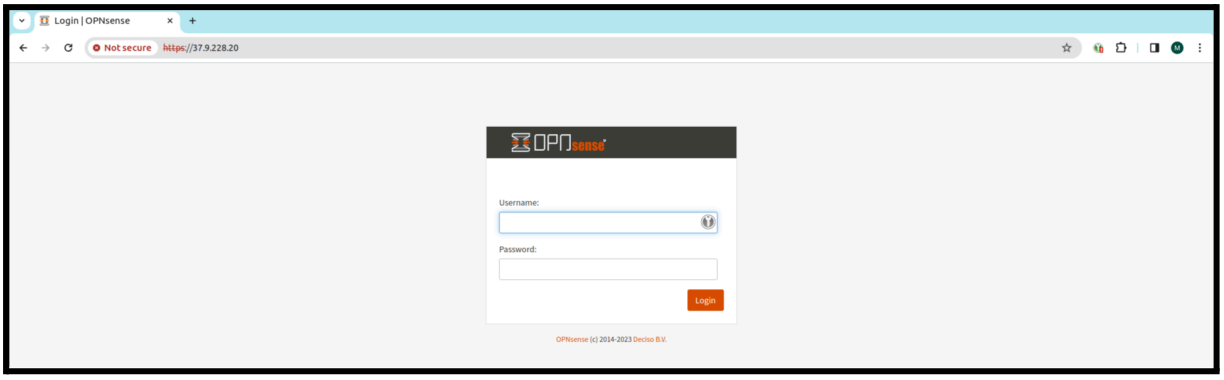
The purpose is to identify security weaknesses as well as the potential impact of such vulnerabilities on the network's resources and data.

The tester uses various methods and tools to simulate an attack on the network, mimicking the actions of a potential attacker. This test helps organizations understand their security posture, identify areas for improvement, and implement strategies to enhance their defenses against real cyber attacks.

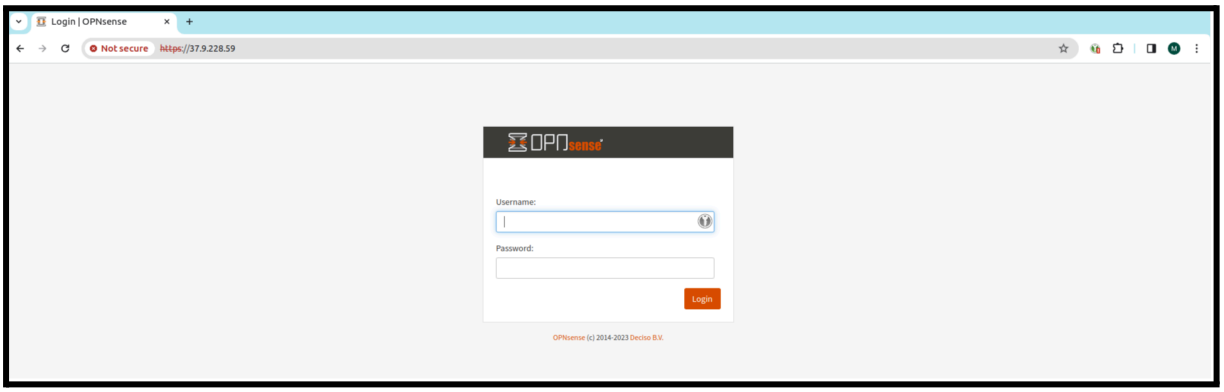
## 3.1 Exposed Administrative Interface (High)

During the analysis, one or more administrative interfaces were found, they should be exposed only to administration networks or trusted IPs.

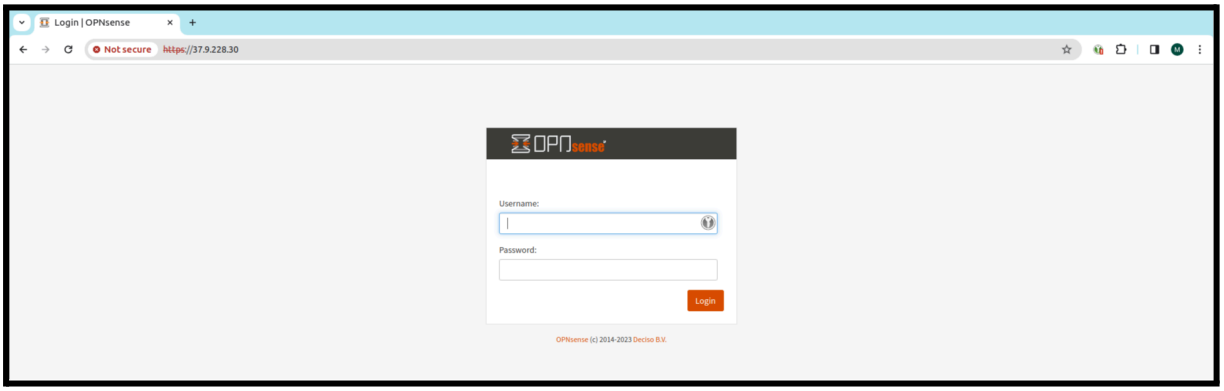
This vulnerability could allow an attacker to use brute-forcing credential tools with the aim to identify weak password patterns or default credentials.



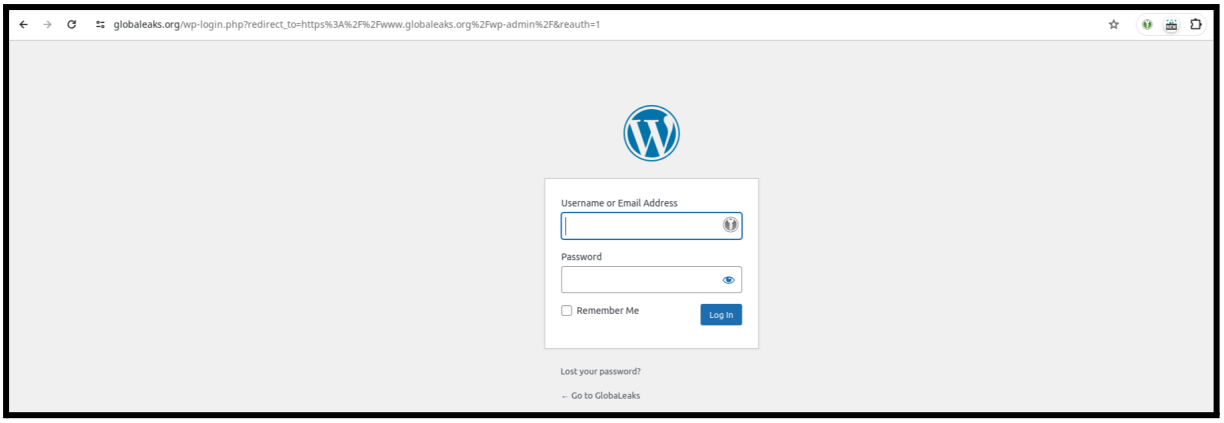

*OPNsense exposed at 37.9.228.20 443/tcp*



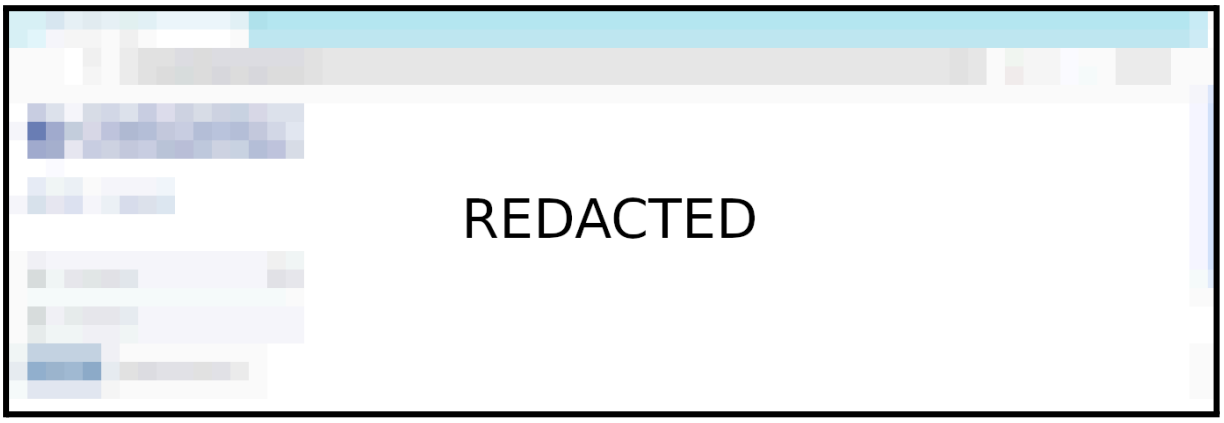

*OPNsense exposed at 37.9.228.59 443/tcp*




*OPNsense exposed at 37.9.228.30 443/tcp*




*WordPress admin panel exposed at https://www.globaleaks.org/wp-login.php*




*Admin interface exposed at -REDACTED-*

**Affected systems**

```
37.9.228.20
37.9.228.59
37.9.228.30
www.globaleaks.org
-REDACTED-
```

**Remedy actions**

• Expose the applications and services only to a trusted management network;
• Alternatively, when system exposure cannot be limited, enable two-factor authentication.

References:

- CWE-419: Unprotected Primary Channel
- A04:2021 – Insecure Design
- The Google Hacking Database (GHDB) community
- Google Hacking Database

## 3.2 Strict Transport Security (HSTS) not enforced (Medium)

The remote HTTPS server is not enforcing HTTP Strict Transport Security (HSTS).

The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections.

```
$ curl -kis https://37.9.228.30/ | head -n 20
HTTP/2 200
set-cookie: PHPSESSID=b1629ad6ebc9e67c89f0827080f0cab9; path=/; secure;
HttpOnly
set-cookie: PHPSESSID=b1629ad6ebc9e67c89f0827080f0cab9; path=/; secure;
HttpOnly
set-cookie: cookie_test=e36ea965c1a1a837d298661890dcb1a3; expires=Fri,
19-Jan-2024 15:50:53 GMT; Max-Age=3600; path=/; secure; HttpOnly
expires: Thu, 19 Nov 1981 08:52:00 GMT
cache-control: no-store, no-cache, must-revalidate
pragma: no-cache
content-security-policy: default-src 'self'; script-src 'self' 'unsafe-inline'
'unsafe-eval'; style-src 'self' 'unsafe-inline' 'unsafe-eval';
x-frame-options: SAMEORIGIN
x-content-type-options: nosniff
x-xss-protection: 1; mode=block
referrer-policy: same-origin
content-type: text/html; charset=UTF-8
accept-ranges: bytes
content-length: 2628
date: Fri, 19 Jan 2024 14:50:53 GMT
server: OPNsense
```

*"Strict-Transport-Security" HTTP header is missing on https://37.9.228.30/*

```
$ curl -kis https://37.9.228.59/ | head -n 20
HTTP/2 200
set-cookie: PHPSESSID=c504e24478daeb03de2c7dd9333f55a9; path=/; secure;
HttpOnly
set-cookie: PHPSESSID=c504e24478daeb03de2c7dd9333f55a9; path=/; secure;
HttpOnly
set-cookie: cookie_test=ffe37f8f9c417d85f1c99ce27616e74c; expires=Fri,
19-Jan-2024 15:53:25 GMT; Max-Age=3600; path=/; secure; HttpOnly
expires: Thu, 19 Nov 1981 08:52:00 GMT
cache-control: no-store, no-cache, must-revalidate
pragma: no-cache
content-security-policy: default-src 'self'; script-src 'self' 'unsafe-inline'
'unsafe-eval'; style-src 'self' 'unsafe-inline' 'unsafe-eval';
x-frame-options: SAMEORIGIN
x-content-type-options: nosniff
x-xss-protection: 1; mode=block
referrer-policy: same-origin
content-type: text/html; charset=UTF-8
accept-ranges: bytes
content-length: 2628
date: Fri, 19 Jan 2024 14:53:25 GMT
server: OPNsense
```

*"Strict-Transport-Security" HTTP header is missing on https://37.9.228.59/*

```
$ curl -kis https://37.9.228.20/ | head -n 20
HTTP/2 200
set-cookie: PHPSESSID=f5812c6188baa33d191d35beb4d464bd; path=/; secure;
HttpOnly
set-cookie: PHPSESSID=f5812c6188baa33d191d35beb4d464bd; path=/; secure;
HttpOnly
set-cookie: cookie_test=07038a512d731fe9e559097f82fe9f36; expires=Fri,
19-Jan-2024 15:58:05 GMT; Max-Age=3600; path=/; secure; HttpOnly
expires: Thu, 19 Nov 1981 08:52:00 GMT
cache-control: no-store, no-cache, must-revalidate
pragma: no-cache
content-security-policy: default-src 'self'; script-src 'self' 'unsafe-inline'
'unsafe-eval'; style-src 'self' 'unsafe-inline' 'unsafe-eval';
x-frame-options: SAMEORIGIN
x-content-type-options: nosniff
x-xss-protection: 1; mode=block
referrer-policy: same-origin
content-type: text/html; charset=UTF-8
accept-ranges: bytes
content-length: 2628
date: Fri, 19 Jan 2024 14:58:05 GMT
server: OPNsense
```

*"Strict-Transport-Security" HTTP header is missing on https://37.9.228.20/*

**Affected systems**

```
37.9.228.20
37.9.228.59
37.9.228.30
```

**Remedy actions**

- Configure the remote web server to use HSTS;
- Set a "max-age" value at least 2592000 (30 days).

References:

- HTTP Strict Transport Security (HSTS)
- CWE-523: Unprotected Transport of Credentials
- Strict-Transport-Security

## 3.3 SSL Self-Signed Certificate (Medium)

The SSL certificate chain for this service ends in an unrecognized self-signed certificate.

The X.509 certificate chain for this service is not signed by a recognized certificate authority.

If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.

```
The following certificate was found at the top of the certificate chain sent by
the remote host, but is self-signed and was not found in the list of known
certificate authorities:

|-Subject : C=NL/ST=Zuid-Holland/L=Middelharnis/O=OPNsense
```

*Evidence for 37.9.228.30 443/tcp*

```
The following certificate was found at the top of the certificate chain sent by
the remote host, but is self-signed and was not found in the list of known
certificate authorities:

|-Subject :
C=IT/ST=Italy/L=Milano/O=GlobaLeaks/E=admin@globaleaks.org/CN=globaleaks
```

*Evidence for 37.9.228.59 443/tcp*

```
The following certificate was found at the top of the certificate chain sent by
the remote host, but is self-signed and was not found in the list of known
certificate authorities:

|-Subject : C=NL/ST=Zuid-Holland/L=Middelharnis/O=OPNsense
```

*Evidence for 37.9.228.20 443/tcp*

**Affected systems**

```
37.9.228.20
37.9.228.59
37.9.228.30
```

**Remedy actions**

- Purchase or generate a proper certificate for this service.

References:

- Self-signed certificate

## 3.4 SSL Certificate Expiry (Medium)

The remote server's SSL certificate has already expired.

```
Subject : C=NL, ST=Zuid-Holland, L=Middelharnis, O=OPNsense
Issuer : C=NL, ST=Zuid-Holland, L=Middelharnis, O=OPNsense
Not valid before : Nov 24 12:58:24 2019 GMT
Not valid after : Nov 23 12:58:24 2020 GMT
```

*The SSL certificate has already expired: 37.9.228.30 443/tcp*

```
Subject : C=NL, ST=Zuid-Holland, L=Middelharnis, O=OPNsense
Issuer : C=NL, ST=Zuid-Holland, L=Middelharnis, O=OPNsense
Not valid before : Nov 24 12:58:24 2019 GMT
Not valid after : Nov 23 12:58:24 2020 GMT
```

*The SSL certificate has already expired: 37.9.228.20 443/tcp*

**Affected systems**

37.9.228.20
37.9.228.30

**Remedy actions**

• Purchase or generate a new SSL certificate to replace the existing one;
• Periodically check the expiration dates of the SSL certificates associated with the enabled services.

## 3.5 Technology or Version Disclosure (Low)

It is possible to obtain information that allows precise identification of the used technologies and software versions, facilitating possible attacks.

```
The remote web server type is: OPNsense
```

*Evidence for 37.9.228.30 443/tcp and 80/tcp*

```
The remote web server type is: OPNsense
```

*Evidence for 37.9.228.20 443/tcp and 80/tcp*

```
The remote web server type is: OPNsense
```

*Evidence for 37.9.228.59 443/tcp and 80/tcp*

```
The remote web server type is: nginx/1.18.0
```

*Evidence for 95.174.23.113 443/tcp and 80/tcp*

**Affected systems**

```
37.9.228.20
37.9.228.59
37.9.228.30
95.174.23.113
```

**Remedy actions**

• Configure the server to avoid sending the versions of the technologies used.

References:

- CWE-200: Exposure of Sensitive Information to an Unauthorized Actor
- A05:2021 – Security Misconfiguration

## 3.6 TLS Version 1.2 Protocol Detection (Info)

The remote service accepts connections encrypted using TLS 1.2.

```
37.9.228.20 443/tcp
37.9.228.30 443/tcp
37.9.228.59 443/tcp
95.174.23.113 443/tcp
95.174.23.113 587/tcp
95.174.28.205 443/tcp
```

*TLSv1.2 is enabled and the server supports at least one cipher*

**Affected systems**

```
37.9.228.30
37.9.228.59
95.174.28.205
95.174.23.113
37.9.228.20
```

**Remedy actions**

- Enable support for TLS 1.3 and disable support for TLS 1.2.

References:

- The Transport Layer Security (TLS) Protocol Version 1.2

## 3.7 TLS Version 1.3 Protocol Detection (Info)

The remote service accepts connections encrypted using TLS 1.3.

```
37.9.228.20 443/tcp
37.9.228.30 443/tcp
37.9.228.59 443/tcp
95.174.23.113 443/tcp
95.174.23.113 587/tcp
95.174.28.205 443/tcp
```

*TLSv1.3 is enabled and the server supports at least one cipher*

**Affected systems**

```
37.9.228.30
37.9.228.59
95.174.28.205
95.174.23.113
37.9.228.20
```

**Remedy actions**

- N/A.

References:

- The Transport Layer Security (TLS) Protocol Version 1.3

PUBLIC DOCUMENT

DISCLOSURE PERMITTED ON CUSTOMER WEBSITE



This activity has been sponsored by Whistleblowing Solutions Impresa Sociale S.r.l..