Network Vulnerability Scanner Report

pentest-ground.com

The Light Network Scanner only ran limited, version-based detection. Upgrade to run Deep scans that check for 20,000+ additional vulnerabilities - with fewer False Positives

Summary

Overall risk level:
Medium

Risk ratings:

Critical:	0
High:	0
Medium:	1
Low:	0
Info:	9

Scan information:

Start time:	Apr 22, 2025 / 12:04:57 UTC+01
Finish time:	Apr 22, 2025 / 12:06:19 UTC+01
Scan duration:	1 min, 22 sec
Tests performed:	10/10
Scan status:	Finished

Findings

Vulnerabilities found for jQuery 3.4.1

port 81/tcp

UNCONFIRMED

Risk level	CVSS	CVE	Summary	Exploit
	4.3	CVE-2020-11023	In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing <option> elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.	N/A
	4.3	CVE-2020-11022	In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.	N/A

Details

Risk description:
These vulnerabilities expose the affected applications to the risk of unauthorized access to confidential data and possibly to denial of service attacks. An attacker could search for an appropriate exploit (or create one) for any of these vulnerabilities and use it to attack the system.

Notes:
- The vulnerabilities are identified based on the server's version.
- Only the first 5 vulnerabilities with the highest risk are shown for each port.

Recommendation:
We recommend you to upgrade the affected software to the latest version in order to eliminate the risks imposed by these vulnerabilities.

IP Information

CONFIRMED

IP Address	Hostname	Location	Autonomous system (AS) Information	Organization (Name & Type)
178.79.134.182	pentest-ground.com	London, England, United Kingdom	Akamai Technologies Inc (AS63949)	Linode LLC (hosting)

Details

Risk description:

If an attacker knows the physical location of an organization's IP address and its Autonomous System (AS) number, they could launch targeted physical or cyber attacks, exploiting regional vulnerabilities or disrupting critical infrastructure.

Recommendation:
We recommend reviewing physical security measures and monitoring network traffic for unusual activity, indicating potential cyber threats. Additionally, implementing robust network segmentation and adopting encryption protocols for data in transit can help protect sensitive information, even if attackers are aware of the IP addresses and the Autonomous System (AS) number.

DNS Records

port 53/udp

CONFIRMED

Domain Queried	DNS Record Type	Description	Value
pentest-ground.com	A	IPv4 address	178.79.134.182
pentest-ground.com	NS	Name server	ns1.linode.com
pentest-ground.com	NS	Name server	ns3.linode.com
pentest-ground.com	NS	Name server	ns5.linode.com
pentest-ground.com	NS	Name server	ns4.linode.com
pentest-ground.com	NS	Name server	ns2.linode.com
pentest-ground.com	MX	Mail server	10 mail.pentest-ground.com
pentest-ground.com	SOA	Start of Authority	ns1.linode.com. admin2.admin.test. 2021000148 14400 14400 1209600 86400
pentest-ground.com	CAA	Certificate Authority Authorization	0 issue "letsencrypt.org"

Details

Risk description:
An initial step for an attacker aiming to learn about an organization involves conducting searches on its domain names to uncover DNS records associated with the organization. This strategy aims to amass comprehensive insights into the target domain, enabling the attacker to outline the organization's external digital landscape. This gathered intelligence may subsequently serve as a foundation for launching attacks, including those based on social engineering techniques. DNS records pointing to services or servers that are no longer in use can provide an attacker with an easy entry point into the network.

Recommendation:
We recommend reviewing all DNS records associated with the domain and identifying and removing unused or obsolete records.

Open ports discovery

CONFIRMED

Port	State	Service	Product	Product Version
80	open	http	nginx	1.27.5
81	open	https	nginx	1.27.5
443	open	https	nginx	1.27.5

Details

Risk description:
This is the list of ports that have been found on the target host. Having unnecessary open ports may expose the target to more risks because those network services and applications may contain vulnerabilities.

Recommendation:
We recommend reviewing the list of open ports and closing the ones which are not necessary for business purposes.

Web redirect detected on port 80

CONFIRMED

We managed to detect the redirect using the following Request / Response chain.

Details

Recommendation:
Vulnerability checks are skipped for ports that redirect to another port. We recommend scanning the redirected port directly.

OS Detection

UNCONFIRMED

Operating System
Linux 4.15 - 5.6

Details

Vulnerability description:
OS Detection

Server software and technologies

port 81/tcp

UNCONFIRMED

Software / Version	Category
Bootstrap	UI frameworks
Nginx 1.27.5	Web servers, Reverse proxies
Cloudflare	CDN
OWL Carousel	JavaScript libraries
jQuery 3.4.1	JavaScript libraries
cdnjs	CDN

Details

Vulnerability description:
We noticed that server software and technology details are exposed, potentially aiding attackers in tailoring specific exploits against identified systems and versions.

Risk description:
The risk is that an attacker could use this information to mount specific attacks against the identified software type and version.

Recommendation:
We recommend you to eliminate the information which permits the identification of software platform, technology, server and operating system: HTTP server headers, HTML meta information, etc.

Server software and technologies

port 443/tcp

UNCONFIRMED

Software / Version	Category
Nginx 1.27.5	Web servers, Reverse proxies
Google Analytics	Analytics

Details

Vulnerability description:
We noticed that server software and technology details are exposed, potentially aiding attackers in tailoring specific exploits against identified systems and versions.

Risk description:
The risk is that an attacker could use this information to mount specific attacks against the identified software type and version.

Recommendation:
We recommend you to eliminate the information which permits the identification of software platform, technology, server and operating system: HTTP server headers, HTML meta information, etc.

Domain name servers are not vulnerable to DNS Server Zone Transfer Information Disclosure (AXFR) vulnerability

Version-based detection found no vulnerabilities for nginx 1.27.5
port 443/tcp

Scan coverage information

List of tests performed (10/10)

- Running IP information lookup phase
- Performing DNS enumeration
- Performing OS detection
- Running port discovery
- Checking for web redirect on port 80
- Attempting zone transfer against name servers...
- Fingerprinting website for technologies on port 81
- Scanning for vulnerabilities of jQuery on port 81
- Fingerprinting website for technologies on port 443
- Searching for version-based vulnerabilities on port 443

Scan parameters

Target:	pentest-ground.com
Preset:	Light
Scanning engines:	Version_based
Check alive:	True
Extensive modules:	-
Protocol type:	TCP
Ports to scan:	Top 100 ports
CVEs:	
Requests per second:	-