Network Vulnerability Scanner Report

✔ **nullclass.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:

Low

Risk ratings:

Critical:	0
High:	0
Medium:	0
Low:	2
Info:	11

Scan information:

Start time:	Jun 20, 2025 / 15:48:00 UTC+0530
Finish time:	Jun 20, 2025 / 15:50:53 UTC+0530
Scan duration:	2 min, 53 sec
Tests performed:	13/13
Scan status:	Finished

Findings

SPF record: Soft-fail ~all configuration

CONFIRMED

Domain Queried	DNS Record Type	Description	Value
nullclass.com	SPF	Sender Policy Framework	"v=spf1 include:_spf.firebasemail.com include:zoho.in include:spf.titan.email include:transmail.net.in include:mailchannels.net ~all"

Details

Vulnerability description:

We found that the Sender Policy Framework (SPF) record for the domain is configured with ~all (soft fail), which indicates that emails from unauthorized IP addresses are not explicitly denied. Instead, the recipient mail server is instructed to treat these messages with suspicion but may still accept them. This configuration may not provide enough protection against email spoofing and unauthorized email delivery, leaving the domain more vulnerable to impersonation attempts.

Risk description:

The ~all directive in an SPF record allows unauthorized emails to pass through some email servers, even though they fail SPF verification. While such emails may be marked as suspicious or placed into a spam folder, not all mail servers handle soft fail conditions consistently. This creates a risk that malicious actors can spoof the domain to send phishing emails or other fraudulent communications, potentially causing damage to the organization's reputation and leading to successful social engineering attacks.

Recommendation:

We recommend changing the SPF record's ~all (soft fail) directive to -all (hard fail). The -all setting tells recipient mail servers to reject emails from any IP addresses not listed in the SPF record, providing stronger protection against email spoofing. Ensure that all legitimate IP addresses and services that send emails on behalf of your domain are properly included in the SPF record before implementing this change.

DKIM record: default selectors found

CONFIRMED

DKIM selector	Key type	Key size	Value
mail	rsa	1296	"k=rsa;p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDeMVIzrCa3T14JsNY0lRv5/2V1/v2itlviLQBwXsa7shBD6TrBkswsFUToPyMRWC9tbR/5ey0nRBH0ZVxp+IsmTxid2Y2z+FApQ6ra2VsXfbJP3HE6wAO0YTVEJt1TmeczhEd2Jiz/fcabIlSgXEdSpTYJhb0ct0VJRxcg4c8c7wIDAQAB"

Details

Vulnerability description:
We found that the DKIM record uses common selectors. The use of common DKIM selectors such as default, test, dkim, or mail may indicate a lack of proper customization or key management. Attackers often target domains using such selectors because they suggest that the domain is relying on default configurations, which could be less secure and easier to exploit. This can increase the risk of DKIM key exposure or misuse.

Risk description:
Using a common DKIM selector makes it easier for attackers to predict and exploit email authentication weaknesses. Attackers may attempt to find corresponding DKIM keys or improperly managed records associated with common selectors. If a common selector is coupled with a weak key length or poor key management practices, it significantly increases the likelihood of email spoofing and phishing attacks.

Recommendation:
We recommend using unique, customized selectors for each DKIM key to make it more difficult for attackers to predict and target the domain's DKIM records. Regularly rotate selectors and associated keys to further strengthen the security of your domain's email authentication infrastructure.

IP Information

CONFIRMED

IP Address	Hostname	Location	Autonomous system (AS) Information	Organization (Name & Type)
172.67.168.218	nullclass.com	-	Cloudflare Inc (AS13335)	Cloudflare Inc (cdn)
104.21.27.31	nullclass.com	-	Cloudflare Inc (AS13335)	Cloudflare Inc (cdn)

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
nullclass.com	A	IPv4 address	104.21.27.31
nullclass.com	A	IPv4 address	172.67.168.218
nullclass.com	NS	Name server	mckinley.ns.cloudflare.com
nullclass.com	NS	Name server	patrick.ns.cloudflare.com
nullclass.com	MX	Mail server	10 mx.zoho.in
nullclass.com	MX	Mail server	20 mx2.zoho.in
nullclass.com	MX	Mail server	50 mx3.zoho.in
nullclass.com	SOA	Start of Authority	mckinley.ns.cloudflare.com. dns.cloudflare.com. 2374093301 10000 2400 604800 1800
nullclass.com	AAAA	IPv6 address	2606:4700:3032::6815:1b1f
nullclass.com	AAAA	IPv6 address	2606:4700:3031::ac43:a8da
nullclass.com	TXT	Text record	"brevo-code:469b188a0fcf390c0c02fe07c28e40b1"
nullclass.com	TXT	Text record	"firebase=nullclassed"

nullclass.com	TXT	Text record	"google-site-verification=6_3Qwae7s2IW48Aj3UFG0TUK7pwY-CskCYglOvfntas"
nullclass.com	TXT	Text record	"zoho-verification=zb18677883.zmverify.zoho.in"
nullclass.com	SPF	Sender Policy Framework	"v=spf1 include:_spf.firebasemail.com include:zoho.in include:spf.titan.email include:transmail.net.in include:mailchannels.net ~all"
nullclass.com	CAA	Certificate Authority Authorization	0 issue "awstrust.com"
nullclass.com	CAA	Certificate Authority Authorization	0 issue "comodoca.com"
nullclass.com	CAA	Certificate Authority Authorization	0 issue "digicert.com; cansignhttpexchanges=yes"
nullclass.com	CAA	Certificate Authority Authorization	0 issue "globalsign.com"
nullclass.com	CAA	Certificate Authority Authorization	0 issue "letsencrypt.org"
nullclass.com	CAA	Certificate Authority Authorization	0 issue "pki.goog; cansignhttpexchanges=yes"
nullclass.com	CAA	Certificate Authority Authorization	0 issue "ssl.com"
nullclass.com	CAA	Certificate Authority Authorization	0 issuewild "comodoca.com"
nullclass.com	CAA	Certificate Authority Authorization	0 issuewild "digicert.com; cansignhttpexchanges=yes"
nullclass.com	CAA	Certificate Authority Authorization	0 issuewild "globalsign.com"
nullclass.com	CAA	Certificate Authority Authorization	0 issuewild "letsencrypt.org"
nullclass.com	CAA	Certificate Authority Authorization	0 issuewild "pki.goog; cansignhttpexchanges=yes"
nullclass.com	CAA	Certificate Authority Authorization	0 issuewild "ssl.com"
_dmarc.nullclass.com	TXT	Text record	"v=DMARC1; p=reject; rua=mailto:79535ef55caa4ffbae6a4bb1e7b7eba8@dmarc-reports.cloudflare.net,mailto:legal@nullclass.com; ruf=mailto:legal@nullclass.com; sp=reject; adkim=s; aspf=s"

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	Cloudflare http proxy	-
443	open	https	cloudflare	-

2082	open	http	Cloudflare http proxy	-
2083	open	https	nginx	-
2086	open	http	Cloudflare http proxy	-
2087	open	https	nginx	-
8080	open	http	Cloudflare http proxy	-
8443	open	http	cloudflare	-

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.

DMARC record is valid and properly configured

CONFIRMED

Domain Queried	DNS Record Type	Description	Value
_dmarc.nullclass.com	TXT	Text record	"v=DMARC1; p=reject; rua=mailto:79535ef55caa4ffbae6a4bb1e7b7eba8@dmarc-reports.cloudflare.net,mailto:legal@nullclass.com; ruf=mailto:legal@nullclass.com; sp=reject; adkim=s; aspf=s"

DKIM records

CONFIRMED

DKIM selector	Key type	Key size	Value
mail	rsa	1296	"k=rsa;p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDeMVIzrCa3T14JsNY0lRv5/2V1/v2itlviLQBwXsa7shBD6TrBkswsFUToPyMRWC9tbR/5ey0nRBH0ZVxp+IsmTxid2Y2z+FApQ6ra2VsXfbJP3HE6wAO0YTVEJt1TmeczhEd2Jiz/fcabIISgXEdSpTYJhb0ct0VJRxcg4c8c7wIDAQAB"

OS Detection

UNCONFIRMED

Operating System	Accuracy
FreeBSD 11.0-STABLE	91%

Details

Vulnerability description:
OS Detection

Server software and technologies

port 443/tcp

UNCONFIRMED

Software / Version	Category
Vercel	PaaS
HSTS	Security

Cloudflare	CDN
HTTP/3	Miscellaneous

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 2083/tcp

UNCONFIRMED

Software / Version	Category
Cloudflare	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 2087/tcp

UNCONFIRMED

Software / Version	Category
Cloudflare	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 8443/tcp

UNCONFIRMED

Software / Version	Category
Cloudflare	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.

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

Scan coverage information

List of tests performed (13/13)

- Performed IP information lookup phase
- Performed DNS enumeration
- Performed OS detection
- Performed port discovery
- Checking for soft-fail ~all configuration in SPF record
- Checking for DMARC policy
- Checking for DKIM records
- Checking for default DKIM selectors
- Attempting zone transfer against name servers...
- Fingerprinted website for technologies
- Fingerprinted website for technologies
- Fingerprinted website for technologies
- Fingerprinted website for technologies

Scan parameters

Target:	nullclass.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:	-