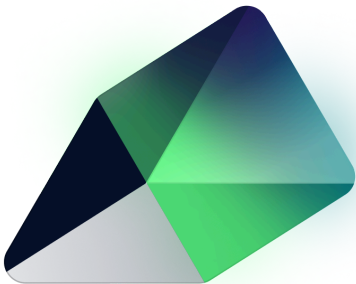


August 5, 2025

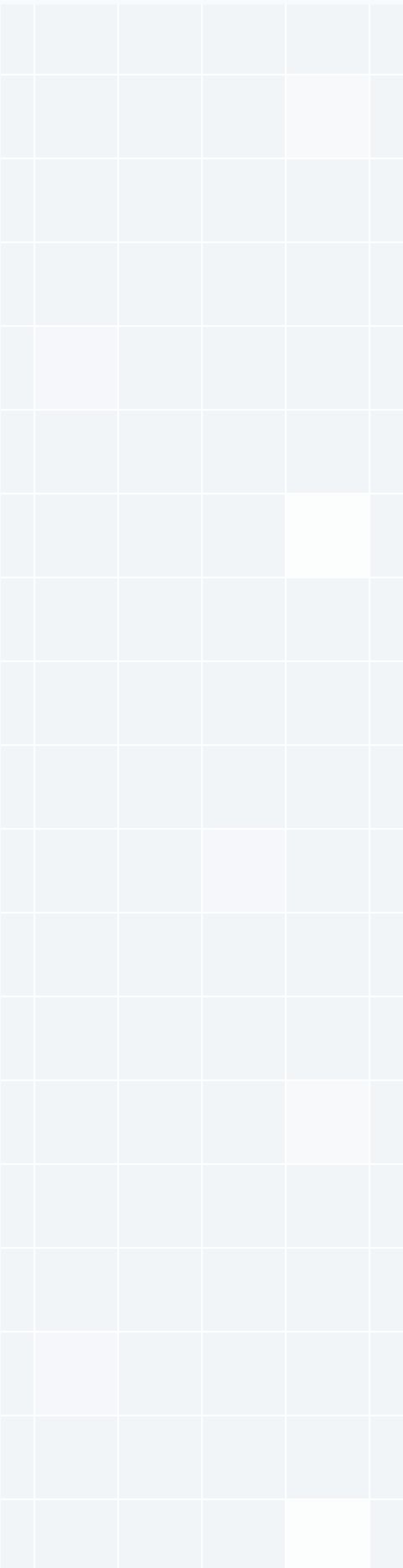
# Vulnerability Scan Report

Prepared By

**HostedScan Security**



hostedscan.com



# Overview

1	Executive Summary	3
2	Trends	4
3	Vulnerabilities By Target	5
4	Open TCP Ports	7
5	Glossary	8

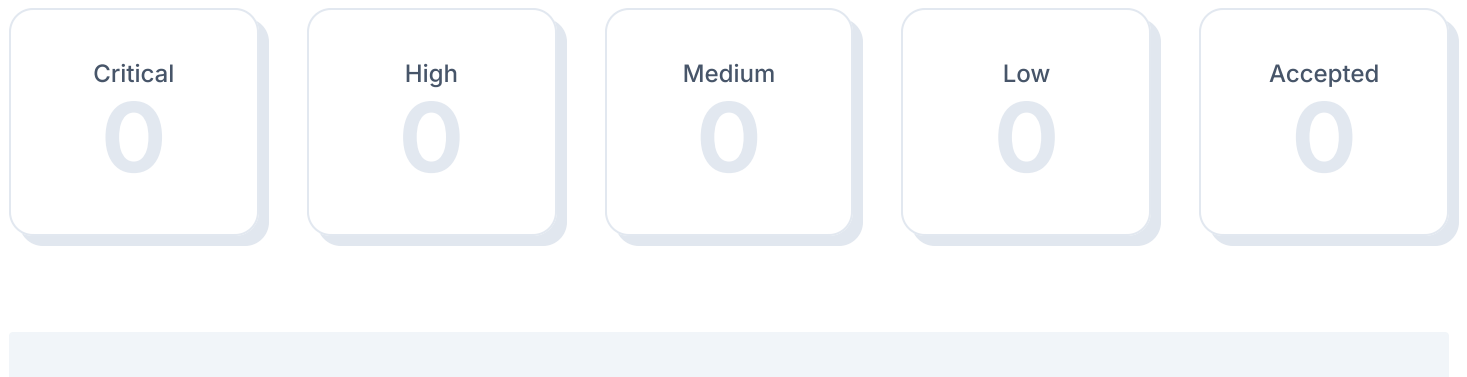


# 1 Executive Summary

Vulnerability scans were conducted on select servers, networks, websites, and applications. This report contains the discovered potential vulnerabilities from these scans. Vulnerabilities have been classified by severity. Higher severity indicates a greater risk of a data breach, loss of integrity, or availability of the targets.

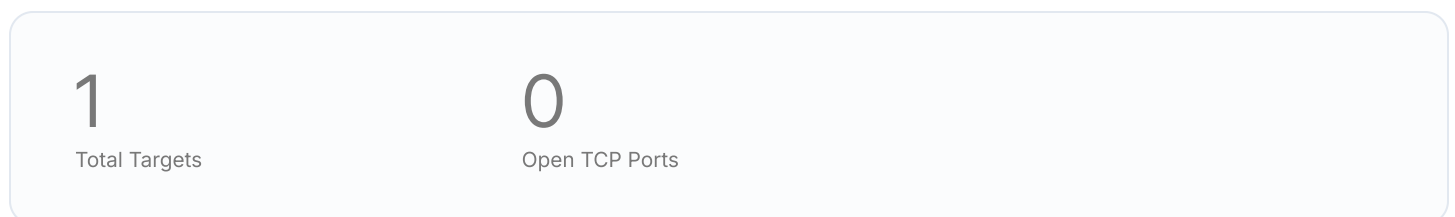
## 1.1 Total Vulnerabilities

Below are the total number of vulnerabilities found by severity. Critical vulnerabilities are the most severe and should be evaluated first. An accepted vulnerability is one which has been manually reviewed and classified as acceptable to not fix at this time, such as a false positive detection or an intentional part of the system's architecture.



## 1.2 Report Coverage

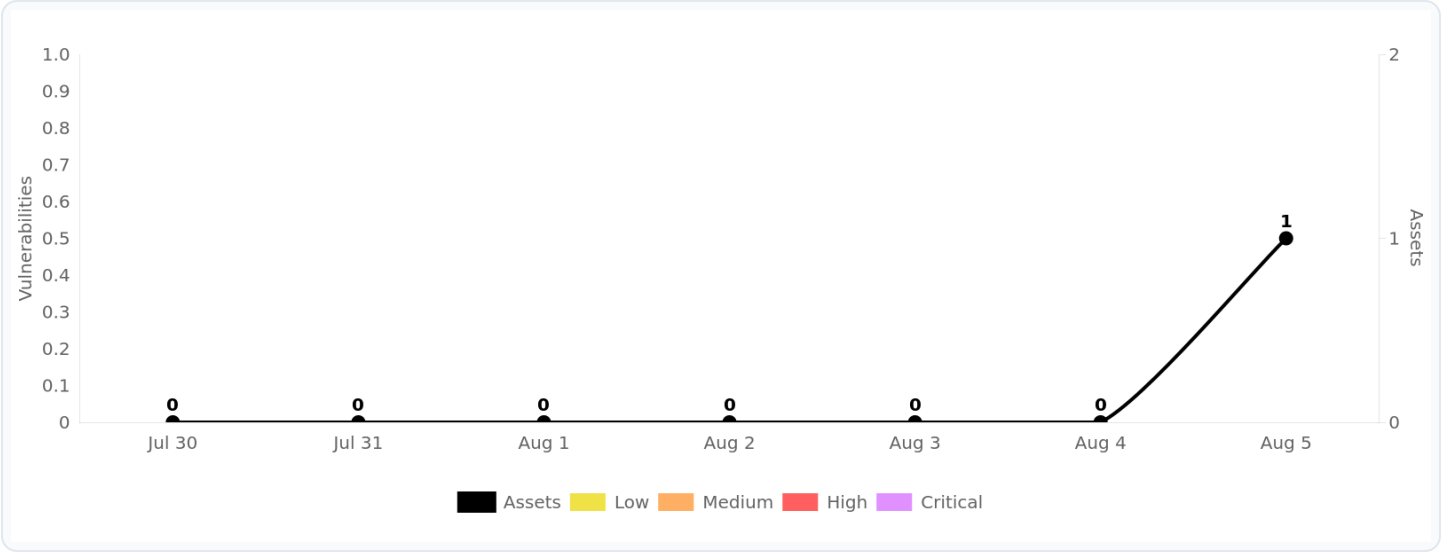
This report includes findings for **1 target** scanned. Each target is a single URL, IP address, or fully qualified domain name (FQDN).



## 2 Trends

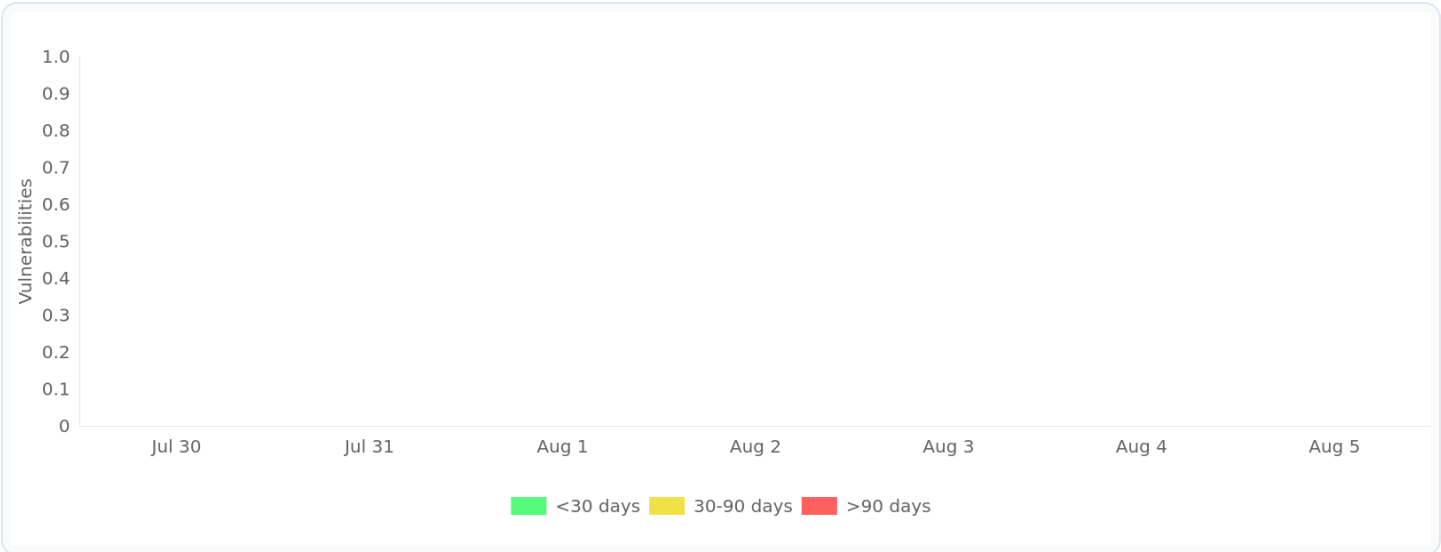
### 2.1 Open Risks

Total number of vulnerabilities grouped by severity level.



### 2.2 Exposure Window

Total number of unresolved vulnerabilities grouped by age (time since first detection).



### 3 Vulnerabilities By Target

This section contains the vulnerability findings for each scanned target. Prioritization should be given to the targets with the highest severity vulnerabilities. However, it is important to take into account the purpose of each system and consider the potential impact a breach or an outage would have for the particular target.


#### 3.1 Targets Summary (1)

The number of potential vulnerabilities found for each target by severity.

Target	<div><div></div>Critical</div>	<div><div></div>High</div>	<div><div></div>Medium</div>	<div><div></div>Low</div>	<div><div></div>Accepted</div>
<div><div></div>208.67.222.226</div>	0	0	0	0	0

### 3.2 Target Breakdowns

Details for the potential vulnerabilities found for each target by scan type.

 208.67.222.226

Total Risks



No vulnerabilities found.

# 4 Open TCP Ports

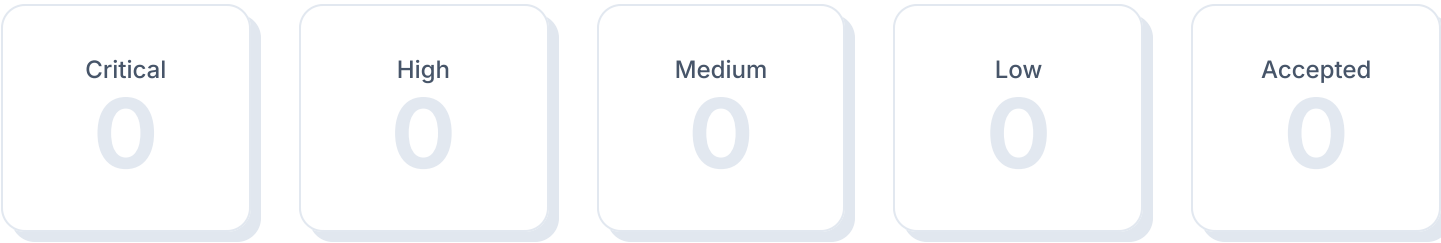
The NMAP TCP port scan discovers open TCP ports with a complete scan of ports 0 to 65535.

## Lite Scan

Free accounts use the lite port scan which is limited to the top 100 most common ports.

## 4.1 Total Vulnerabilities

Total number of vulnerabilities found by severity.



## 4.2 Vulnerabilities Breakdown

Summary list of all detected vulnerabilities.

Title	Severity	Open	Accepted
No vulnerabilities detected			

## 5 Glossary

### Accepted Vulnerability

An accepted vulnerability is one which has been manually reviewed and classified as acceptable to not fix at this time, such as a false positive scan result or an intentional part of the system's architecture.

### Fully Qualified Domain Name (FQDN)

A fully qualified domain name is a complete domain name for a specific website or service on the internet. This includes not only the website or service name, but also the top-level domain name, such as .com, .org, .net, etc. For example, 'www.example.com' is an FQDN.

### Open TCP Ports

The NMAP TCP port scan discovers open TCP ports with a complete scan of ports 0 to 65535.

### Vulnerability

A weakness in the computational logic (e.g., code) found in software and hardware components that, when exploited, results in a negative impact to confidentiality, integrity, or availability. Mitigation of the vulnerabilities in this context typically involves coding changes, but could also include specification changes or even specification deprecations (e.g., removal of affected protocols or functionality in their entirety).

### Target

A target represents target is a single URL, IP address, or fully qualified domain name (FQDN) that was scanned.

### Severity

Severity represents the estimated impact potential of a particular vulnerability. Severity is divided into 5 categories: Critical, High, Medium, Low and Accepted.

### CVSS Score

The CVSS 3.0 score is a global standard for evaluating vulnerabilities with a 0 to 10 scale. CVSS maps to threat levels:

0.1 - 3.9 = Low

4.0 - 6.9 = Medium

7.0 - 8.9 = High

9.0 - 10.0 = Critical

### EPSS Score

The EPSS score is the estimated probability that a given vulnerability will be exploited in the wild within the next 30 days, on a 0% to 100% scale.



This report was prepared using

## HostedScan Security®

For more information, visit [hostedscan.com](https://hostedscan.com)

Founded in Seattle, Washington in 2019, HostedScan, LLC. is dedicated to making continuous vulnerability scanning and risk management much more easily accessible to more businesses.



HostedScan, LLC.

2212 Queen Anne Ave N  
Suite #521  
Seattle, WA 98109

Terms & Policies  
[hello@hostedscan.com](mailto:hello@hostedscan.com)