August 7, 2025

Vulnerability Scan
Report

Prepared By

HostedScan Security

hostedscan.com

Overview

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.

Critical	High	Medium	Low	Accepted
0	0	0	1	0

100%

1.2 Report Coverage

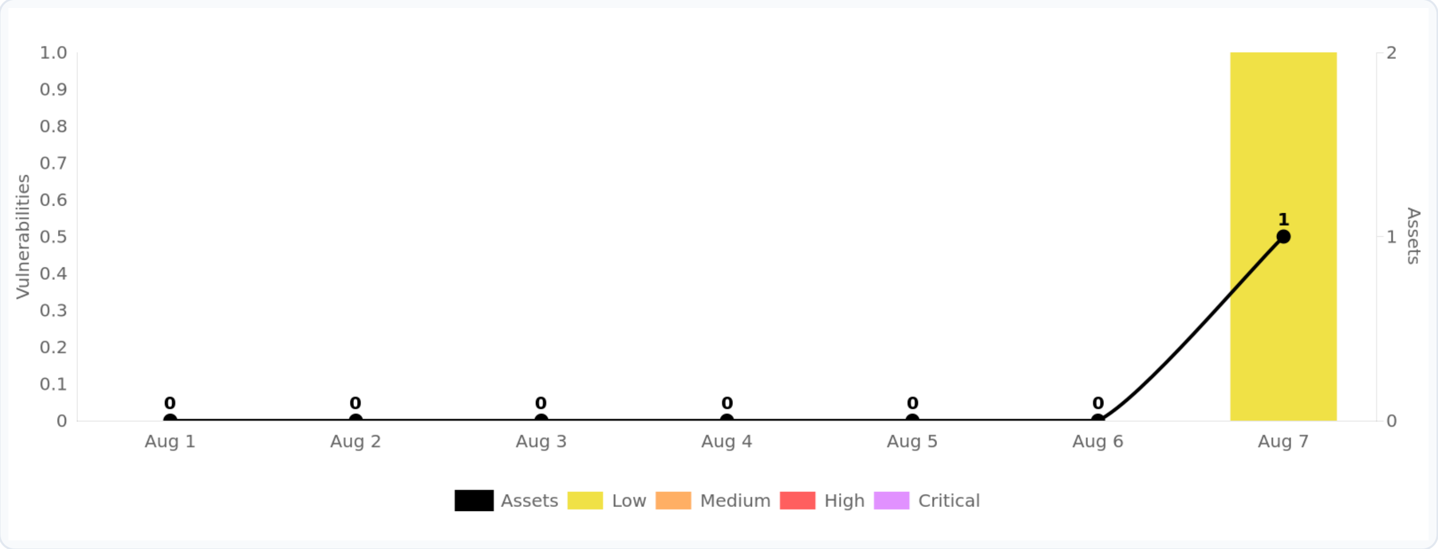
This report includes findings for **1 target** scanned. Each target is a single URL, IP address, or fully qualified domain name (FQDN).

1	1
Total Targets	Network Vulnerabilities

2 Trends

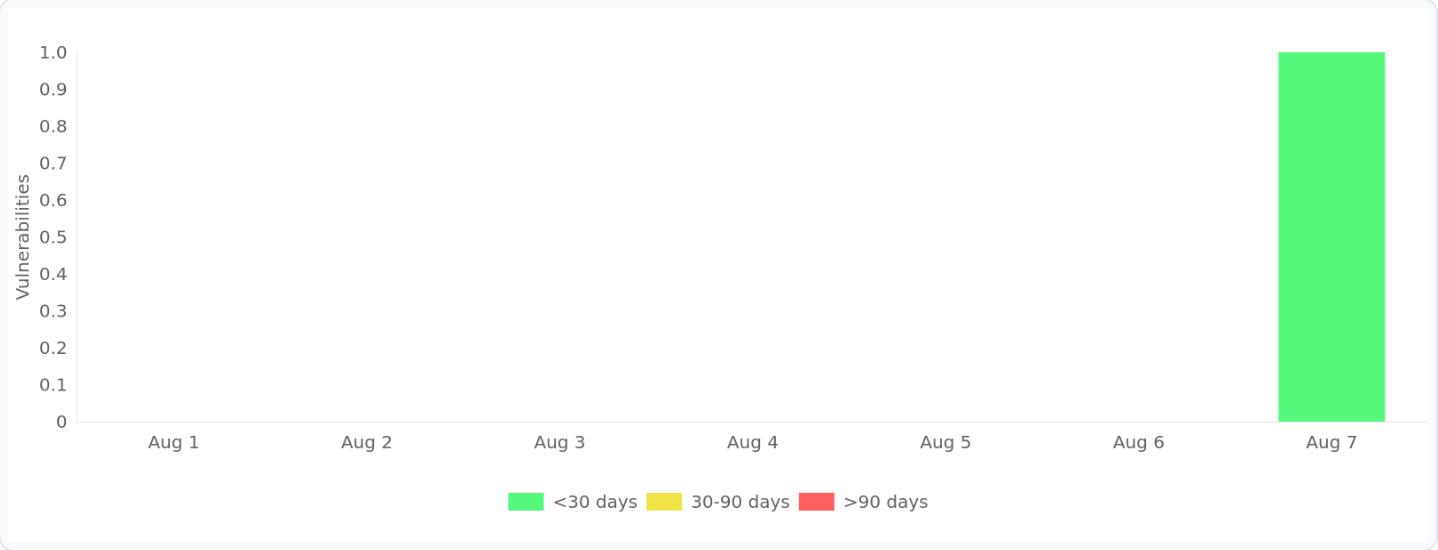
2.1 Open Risks

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	● Critical	● High	● Medium	● Low	● Accepted
● https://www.blueorigin.com/	0	0	0	1	0

3.2 Target Breakdowns

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

https://www.blueorigin.com/

Total Risks

0	0	0	1	0

100%

Network Vulnerabilities	Severity	First Detected	Last Detected
TCP Timestamps Information Disclosure cvss score: 2.6	● Low	0 days ago	0 days ago

4 Network Vulnerabilities

The OpenVAS network vulnerability scan tests servers and internet connected devices for over 150,000 vulnerabilities. OpenVAS uses the Common Vulnerability Scoring System (CVSS) to quantify the severity of findings. 0.0 is the lowest severity and 10.0 is the highest.

Lite Scan

Free accounts use the lite network scan which is limited to the 10 most common ports and excludes brute force tests.

4.1 Total Vulnerabilities

Total number of vulnerabilities found by severity.

Critical	High	Medium	Low	Accepted
0	0	0	1	0

100%

4.2 Vulnerabilities Breakdown

Summary list of all detected vulnerabilities.

Title	Severity	CVSS Score	Open	Accepted
TCP Timestamps Information Disclosure	● Low	2.6	1	0

4.3 Vulnerability Details

Detailed information about each potential vulnerability found by the scan.

TCP Timestamps Information Disclosure

SEVERITY	AFFECTED TARGETS	LAST DETECTED	CVSS SCORE	PORT
Low	1 target	0 days ago	2.6	general/tcp

Description

The remote host implements TCP timestamps and therefore allows to compute the uptime.

The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.

A side effect of this feature is that the uptime of the remote host can sometimes be computed.

It was detected that the host implements RFC1323/RFC7323.

The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 1754307736
Packet 2: 1756974783

Solution

To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.

To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled'

Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled.

The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment.

See the references for more information.

References

https://datatracker.ietf.org/doc/html/rfc1323
https://datatracker.ietf.org/doc/html/rfc7323
https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152
https://www.fortiguard.com/psirt/FG-IR-16-090

Vulnerable Target	First Detected	Last Detected
https://www.blueorigin.com/	0 days ago	0 days ago

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.

Network Vulnerabilities

The OpenVAS network vulnerability scan tests servers and internet connected devices for over 150,000 vulnerabilities. OpenVAS uses the Common Vulnerability Scoring System (CVSS) to quantify the severity of findings. 0.0 is the lowest severity and 10.0 is the highest.

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**

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