September 4, 2023

Vulnerability Scan Report

prepared by

HostedScan Security

hostedscan.com

Overview

1 Executive Summary

Vulnerability scans were conducted on selected servers, networks, websites, and applications. This report contains the discovered potential risks from these scans. Risks have been classified into categories according to the level of threat and degree of potential harm they may pose.

1.1 Total Risks

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

Critical	High	Medium	Low	Accepted
0	1	1	2	0

1.2 Report Coverage

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

Vulnerability Categories

4

Network Vulnerabilities

2 Risks By Target

This section contains the vulnerability findings for each target that was scanned. Prioritize the most vulnerable assets first.

2.1 Targets Summary

The total number of risks found for each target, by severity.

Target	Critical	High	Medium	Low	Accepted
https://www.hindustantimes.com/	0	1	1	2	0

2.2 Target Breakdowns

The risks discovered for each target.

Target
https://www.hindustantimes.com/

Total Risks

0	1	1	2	0

Network Vulnerabilities	Threat Level	First Detected
SSL/TLS: Report Vulnerable Cipher Suites for HTTPS cvss score: 7.5	High	0 days ago
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection cvss score: 4.3	Medium	0 days ago
TCP Timestamps Information Disclosure cvss score: 2.6	Low	0 days ago
ICMP Timestamp Reply Information Disclosure cvss score: 2.1	Low	0 days ago

3 Network Vulnerabilities

The OpenVAS network vulnerability scan tests servers and internet connected devices for over 50,000 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.

3.1 Total Risks

Total number of risks found by severity.

Critical	High	Medium	Low	Accepted
0	1	1	2	0

3.2 Risks Breakdown

Summary list of all detected risks.

Title	Threat Level	CVSS Score	Open	Accepted
SSL/TLS: Report Vulnerable Cipher Suites for HTTPS	High	7.5	1	0
SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	Medium	4.3	1	0
TCP Timestamps Information Disclosure	Low	2.6	1	0
ICMP Timestamp Reply Information Disclosure	Low	2.1	1	0

3.3 Full Risk Details

Detailed information about each risk found by the scan.

SSL/TLS: Report Vulnerable Cipher Suites for HTTPS

High
cvss score: 7.5

Description

This routine reports all SSL/TLS cipher suites accepted by a service where attack vectors exists only on HTTPS services.

These rules are applied for the evaluation of the vulnerable cipher suites:

- 64-bit block cipher 3DES vulnerable to the SWEET32 attack (CVE-2016-2183).

Solution

The configuration of this services should be changed so that it does not accept the listed cipher suites anymore.

Please see the references for more resources supporting you with this task.

References

CVE-2016-2183
CVE-2016-6329
CVE-2020-12872
https://bettercrypto.org/
https://mozilla.github.io/server-side-tls/ssl-config-generator/
https://sweet32.info/

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

SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection

Medium
cvss score: 4.3

Description

It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.

The TLSv1.0 and TLSv1.1 protocols contain known cryptographic flaws like:

- CVE-2011-3389: Browser Exploit Against SSL/TLS (BEAST)

- CVE-2015-0204: Factoring Attack on RSA-EXPORT Keys Padding Oracle On Downgraded Legacy Encryption (FREAK)

An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection.

Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.

Solution

It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.

References

CVE-2011-3389
CVE-2015-0204
https://ssl-config.mozilla.org/
https://bettercrypto.org/
https://datatracker.ietf.org/doc/rfc8996/
https://vnhacker.blogspot.com/2011/09/beast.html
https://web.archive.org/web/20201108095603/https://censys.io/blog/freak
https://www.enisa.europa.eu/publications/algorithms-key-size-and-parameters-report-2014

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

TCP Timestamps Information Disclosure

Low
cvss score: 2.6

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.

Solution

To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps

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

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

ICMP Timestamp Reply Information Disclosure

Low
cvss score: 2.1

Description

The remote host responded to an ICMP timestamp request.

The Timestamp Reply is an ICMP message which replies to a Timestamp message. It consists of the originating timestamp sent by the sender of the Timestamp as well as a receive timestamp and a transmit timestamp.

This information could theoretically be used to exploit weak time-based random number generators in other services.

Solution

Various mitigations are possible:

- Disable the support for ICMP timestamp on the remote host completely

- Protect the remote host by a firewall, and block ICMP packets passing through the firewall in either direction (either completely or only for untrusted networks)

References

CVE-1999-0524
https://datatracker.ietf.org/doc/html/rfc792
https://datatracker.ietf.org/doc/html/rfc2780

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

4 Glossary

Accepted Risk

An accepted risk is one which has been manually reviewed and classified as acceptable to not fix at this time, such as a false positive 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 50,000 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.

Risk

A risk is a finding from a vulnerability scan. Each risk is a potential security issue that needs review. Risks are assigned a threat level which represents the potential severity.

Target

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

Threat Level

The threat level represents the estimated potential severity of a particular risk. Threat level is divided into 4 categories: High, Medium, Low and Accepted.

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