Scanly Scan Report

Network Vulnerability

November 10, 2020 – 4:56pm

Generated by Luke Wallis: wallisl2@example.com

Summary

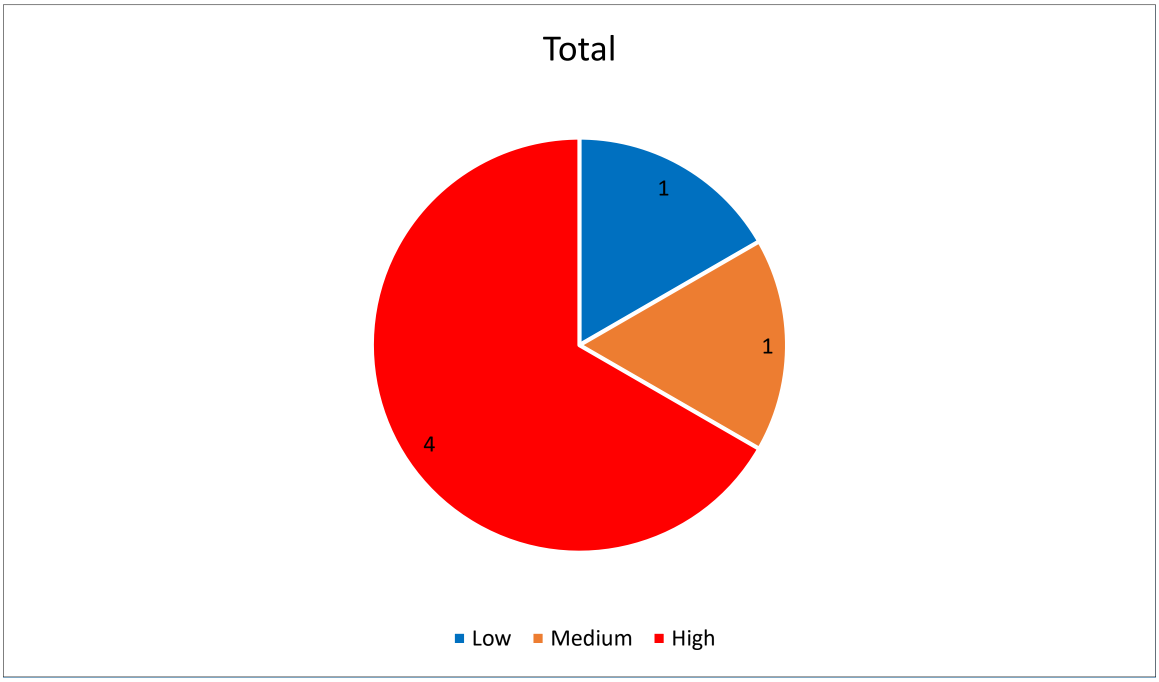
This report was generated by Scanly by DuckDuckGroup.

Contents

1 Result Overview

IP Addresses Scanned	192.168.10.1-2

1.1 Severity Overview



2 Individual Host Overview

2.1 192.168.10.1

Service (Port)	Severity
80 tcp	High
21 tcp	High
22 tcp	Low

2.1.1 80 | TCP | High

Summary

The host is running an outdated version of Apache2.

Installed version: 1.3
Latest Release: 2.4.46

Impact

Exploitation will allow intruders to gain administrative privileges.

Solution

Upgrade Apache2 to the latest release.

2.1.2 21 | TCP | High

Summary

It was possible to login tonto the remote FTP server using weak credentials.

Service is using default credentials.

Impact

Unchallenged remote login to the FTP server.

Solution

Change the credentials as soon as possible.

2.1.3 22 | TCP | Low

Summary

SSH Server is configured to allow weak MD5 algorithms

Impact

Weak client-to-server algorithms may allow attackers to crack SSH logins.

Solution

Disable weak MD5 algorithms.

2.2 192.168.10.2

Service (Port)	Severity
3306 tcp	High
21 tcp	High
23 tcp	Medium

2.2.1 3306 | TCP | High

Summary

It was possible to log into the remote MySQL service as root using weak credentials.

Impact

Attackers can log into MySQL and execute commands as root.

Solution

Change the password as soon as possible.

2.2.2 32 | TCP | High

Summary

It was possible to login tonto the remote FTP server using weak credentials.

Service is using default credentials.

Impact

Unchallenged remote login to the FTP server.

Solution

Change the credentials as soon as possible.

2.2.3 23 | TCP | Medium

Summary

The host is running Telnet which allows cleartext logins over unencrypted connections.

Impact

An attacker can sniff traffic to find usernames and passwords.

Solution

Replace Telnet with a protocol that supports encrypted connections, such as SSH.