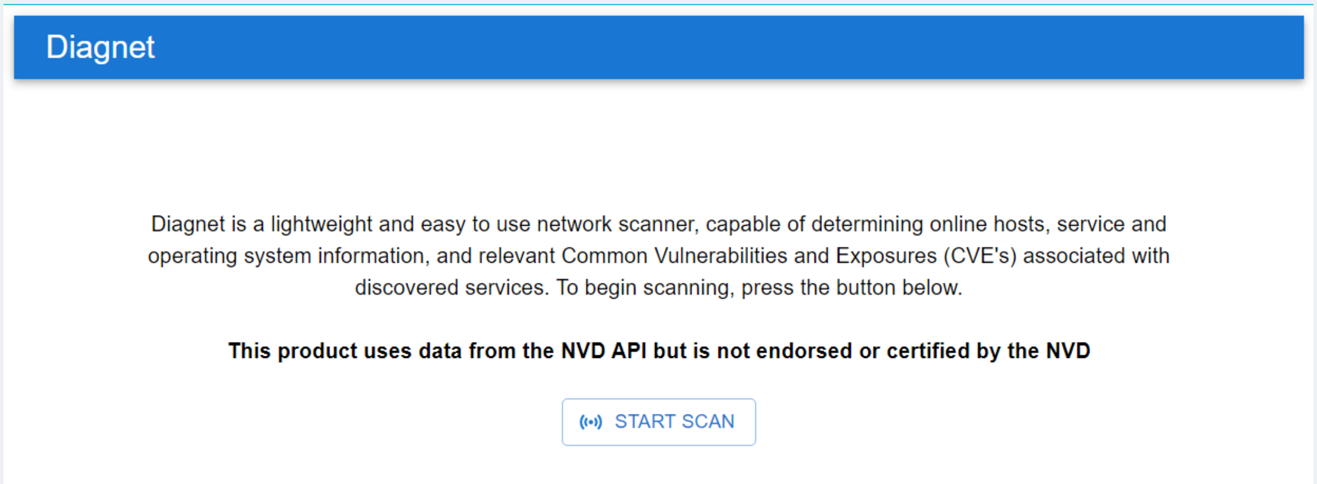
Diagnet
User Guide

INSTRUCTIONS

Diagnet is a simple to use network scanner, capable of identifying vulnerable services. The landing page of the application is displayed below:



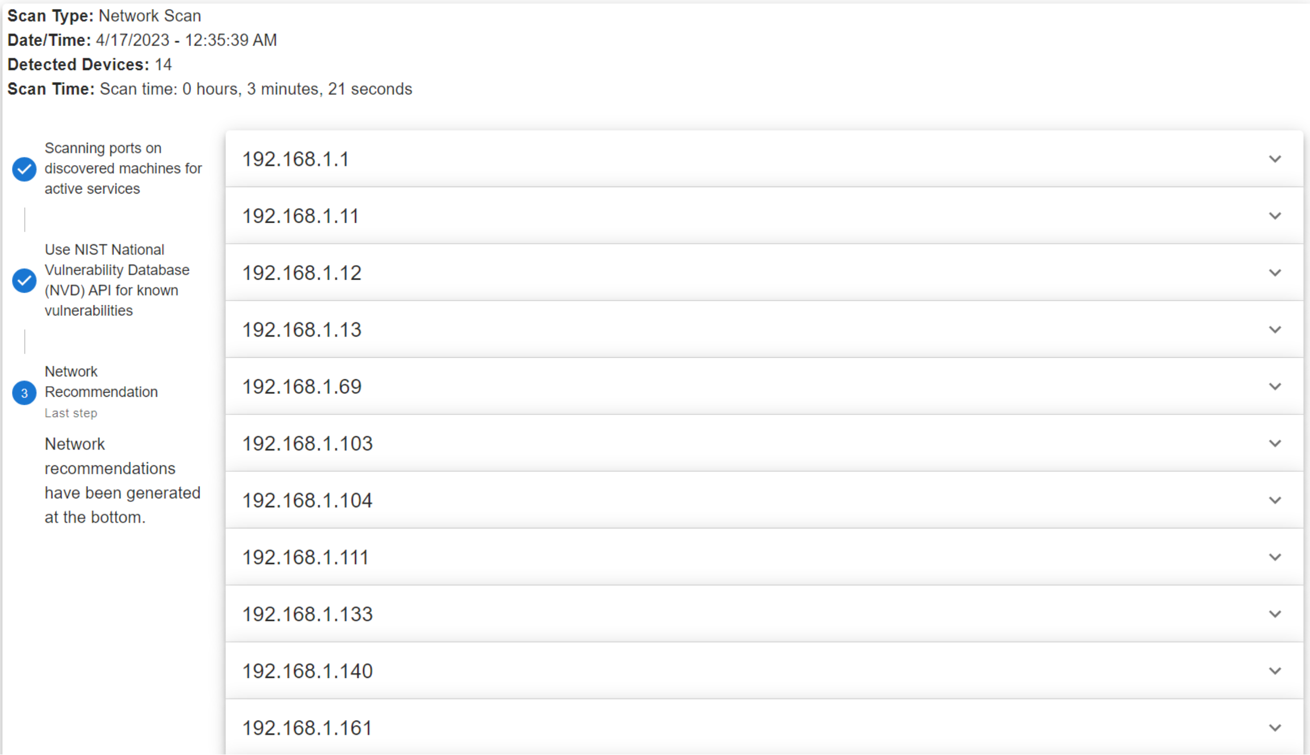
Diagnet is a lightweight and easy to use network scanner, capable of determining online hosts, service and operating system information, and relevant Common Vulnerabilities and Exposures (CVE's) associated with discovered services. To begin scanning, press the button below.

This product uses data from the NVD API but is not endorsed or certified by the NVD

To begin the scan, press **START SCAN**.

Wait for the scan to complete, this process typically takes between 3 – 5 minutes.

Once the scan is complete, the following will be displayed:



Scan Type: Network Scan
Date/Time: 4/17/2023 - 12:35:39 AM
Detected Devices: 14
Scan Time: Scan time: 0 hours, 3 minutes, 21 seconds

✓ Scanning ports on discovered machines for active services

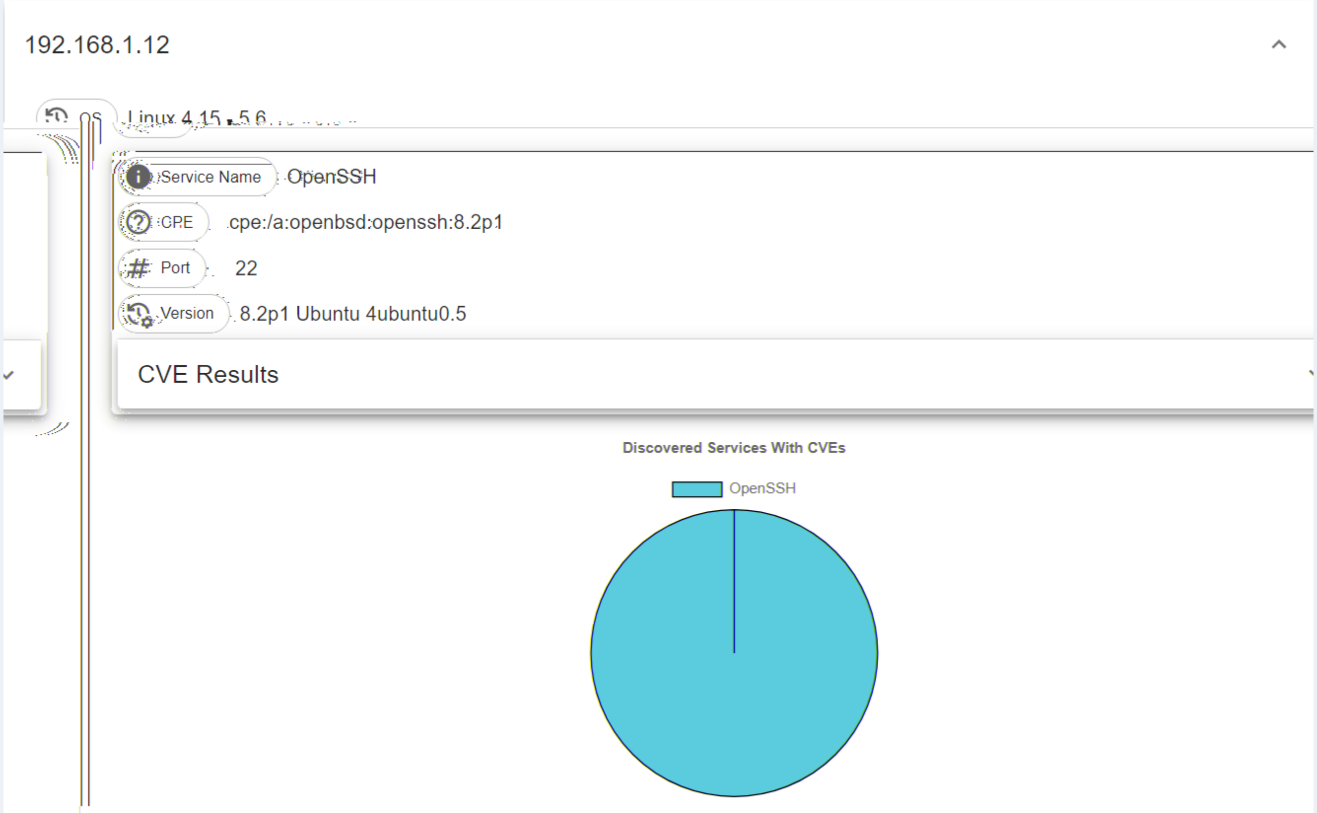
✓ Use NIST National Vulnerability Database (NVD) API for known vulnerabilities

3 Network Recommendation
Last step

Network recommendations have been generated at the bottom.

- 192.168.1.1
- 192.168.1.11
- 192.168.1.12
- 192.168.1.13
- 192.168.1.69
- 192.168.1.103
- 192.168.1.104
- 192.168.1.111
- 192.168.1.133
- 192.168.1.140
- 192.168.1.161

The result is a list of dropdowns, each corresponding to a single IP address. Upon opening a dropdown, the following is displayed:



192.168.1.12

OS Linux 4.15 - 5.6

Service Name OpenSSH

CPE cpe:/a:openbsd:openssh:8.2p1

Port 22

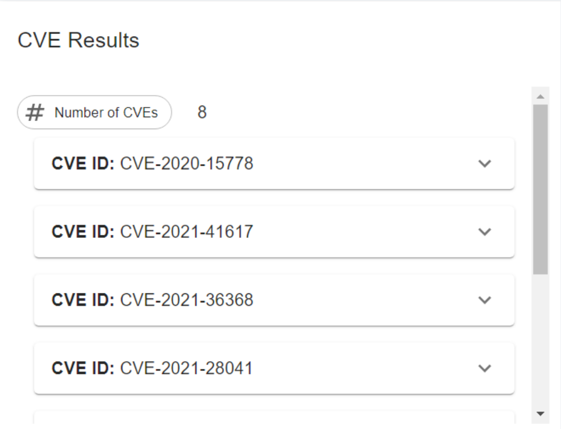
Version 8.2p1 Ubuntu 4ubuntu0.5

CVE Results

Information captured during the scan is displayed, such as:

- Operating System
- Identified Services:
  - Service Name
  - Common Platform Enumeration (CPE)
  - Port
  - Version
- CVE Results Dropdown.
- Graph comparing discovered vulnerable services.

Upon opening the CVE results dropdown, the user is met with a list of all the Common Vulnerabilities and Exposures identified during the scan:



CVE Results

Number of CVEs 8

CVE ID: CVE-2020-15778

CVE ID: CVE-2021-41617

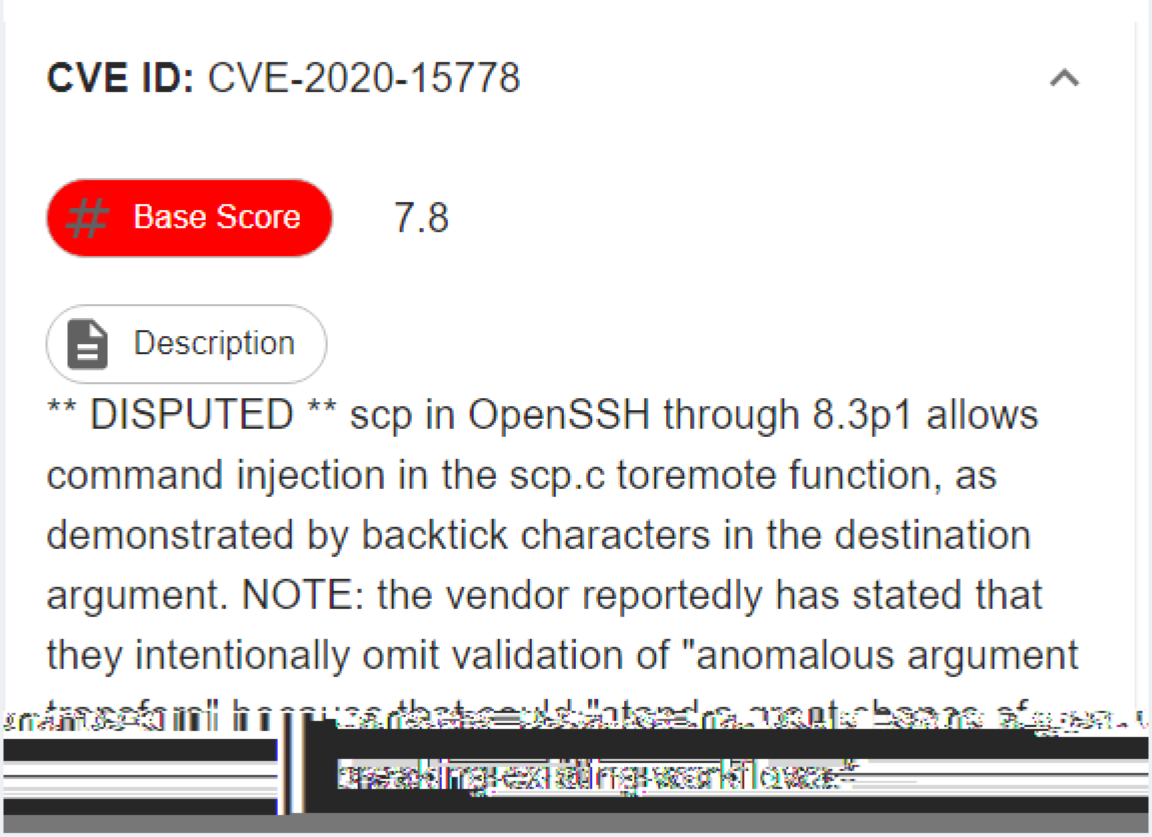
CVE ID: CVE-2021-36368

CVE ID: CVE-2021-28041

Displayed is the following:

- Number of CVEs found.
- CVE ID.

Upon opening a CVE item's dropdown, the following is displayed:



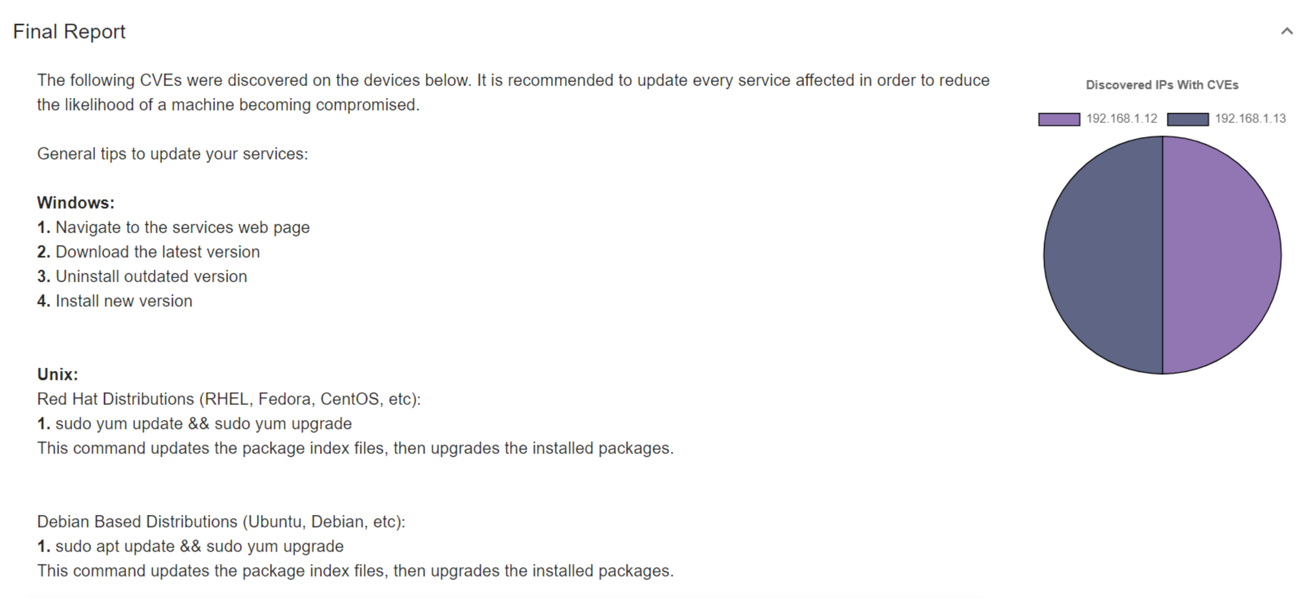
7.8

** DISPUTED ** scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of "anomalous argument transfers" because that could "stand a great chance of breaking existing workflows."

Displayed is the following:

- Base Score: Identifies the severity of the exploit according to the National Institute of Standards and Technology (NIST)
- Description: A brief description of the associated CVE.

At the end of the scan, a dynamically generated report of the findings is displayed:



Final Report

The following CVEs were discovered on the devices below. It is recommended to update every service affected in order to reduce the likelihood of a machine becoming compromised.

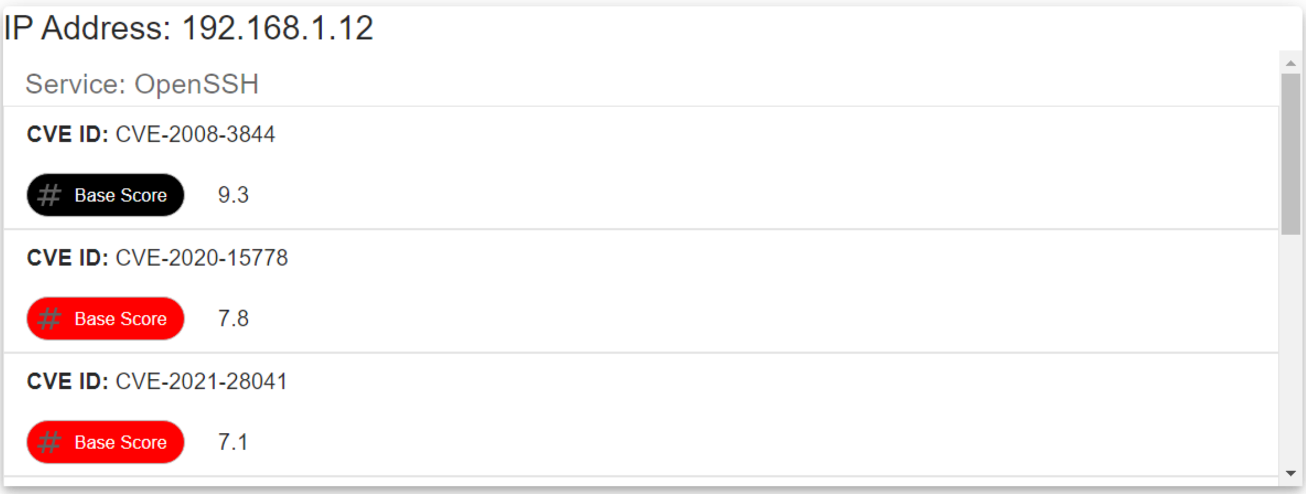
General tips to update your services:

Windows:
1. Navigate to the services web page
2. Download the latest version
3. Uninstall outdated version
4. Install new version

Unix:
Red Hat Distributions (RHEL, Fedora, CentOS, etc):
1. sudo yum update && sudo yum upgrade
This command updates the package index files, then upgrades the installed packages.

Debian Based Distributions (Ubuntu, Debian, etc):
1. sudo apt update && sudo yum upgrade
This command updates the package index files, then upgrades the installed packages.

A list of all CVEs are also displayed alongside the report:



IP Address: 192.168.1.12

Service: OpenSSH

CVE ID: CVE-2008-3844

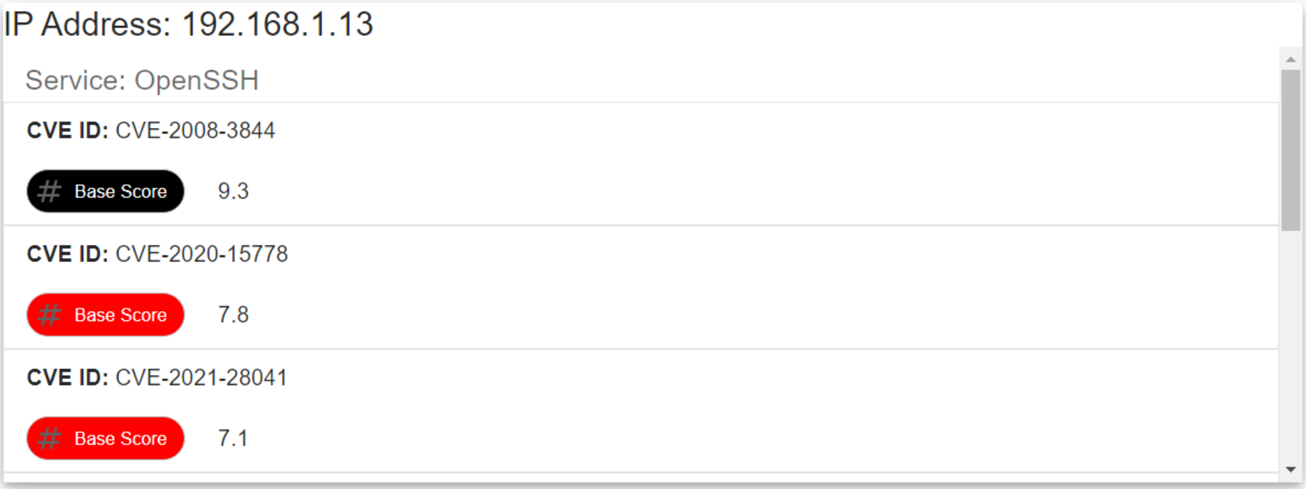
Base Score 9.3

CVE ID: CVE-2020-15778

Base Score 7.8

CVE ID: CVE-2021-28041

Base Score 7.1



IP Address: 192.168.1.13

Service: OpenSSH

CVE ID: CVE-2008-3844

Base Score 9.3

CVE ID: CVE-2020-15778

Base Score 7.8

CVE ID: CVE-2021-28041

Base Score 7.1