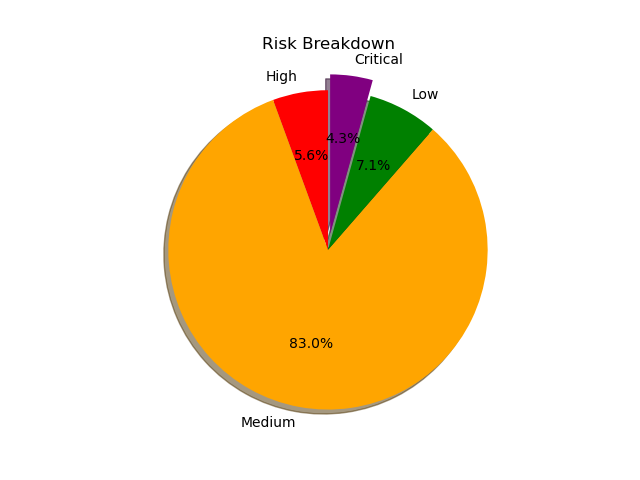
### Risk Summary

The breakdown of the vulnerabilities is as follows: Critical Vulnerabilities account for 4.3% of the total vulnerabilities, High Vulnerabilities account for 5.59% of the total vulnerabilities, Medium Vulnerabilities account for 83.01% of the total vulnerabilities, Low Vulnerabilities account for 7.1% of the total vulnerabilities.   
Highest risk is Medium

### Risk Break down



### Host Breakdown

The host with the highest risk is 192.168.1.4 with 33 vulnerabilities,which accounts for 7.1% of the total vulnerabilities.  
The Top 5 hosts with the most vulnerabilities are: ['192.168.1.1', '192.168.1.4', '192.168.1.5', '192.168.1.9', '192.168.1.11'] with [3, 33, 12, 11, 2] vulnerabilities which accounts for 13.12% of the total vulnerabilities respectively.

### Common Vulnerabilities

The most common vulnerability is SSL Certificate Cannot Be Trusted with 98 occurences and a risk of Medium. Its solution is to Purchase or generate a proper SSL certificate for this service.  
The second most common vulnerability is SSL Self-Signed Certificate with 87 occurences and a risk of Medium. Its solution is to Purchase or generate a proper SSL certificate for this service.  
The third most common vulnerability is SSL Certificate Expiry with 40 occurences

### Critical Vulnerabilities

The vulnerability with Critical risk is SSL Version 2 and 3 Protocol Detection with 8 occurencesand a risk of Critical. Its solution is to Consult the application's documentation to disable SSL 2.0 and 3.0.  
Use TLS 1.2 (with approved cipher suites) or higher instead.   
The Second Highest Critical vulnerability is Multiple Command Injection Vulnerabilities in Grandstream Products with 6 occurences and a risk of Critical. Its solution is to Update to the fixed version as per the advisory.   
The Third Highest Critical vulnerability is phpMyAdmin 4.x 4.8.5 Multiple Vulnerabilities (PMASA-2019-1) (PMASA-2019-2) with 4 occurences and a risk of Critical. Its solution is to Upgrade to phpMyAdmin version 4.8.5 or later.  
Alternatively, apply the patches referenced in the vendor advisories.