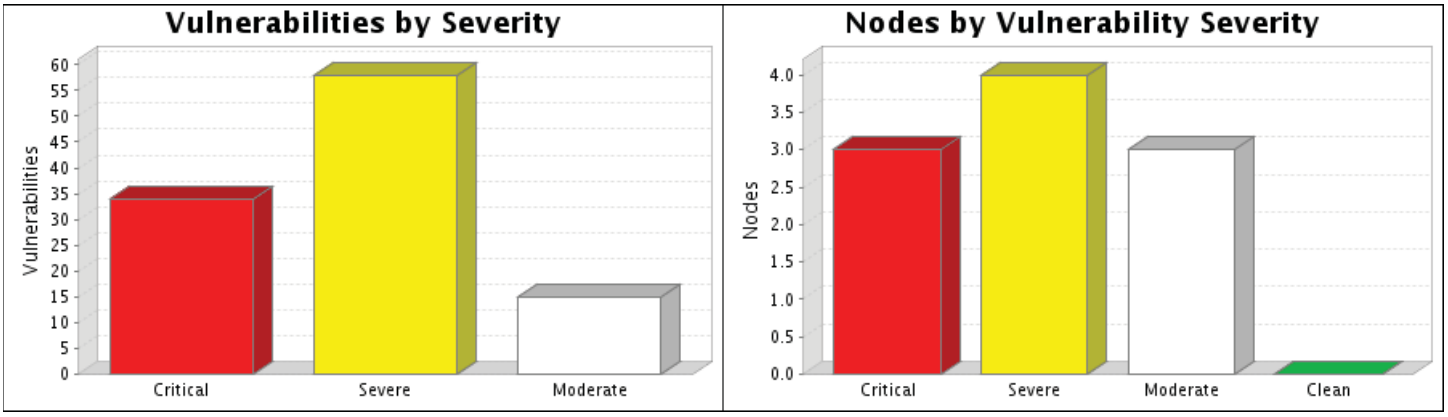
Executive Overview

1. Executive Summary

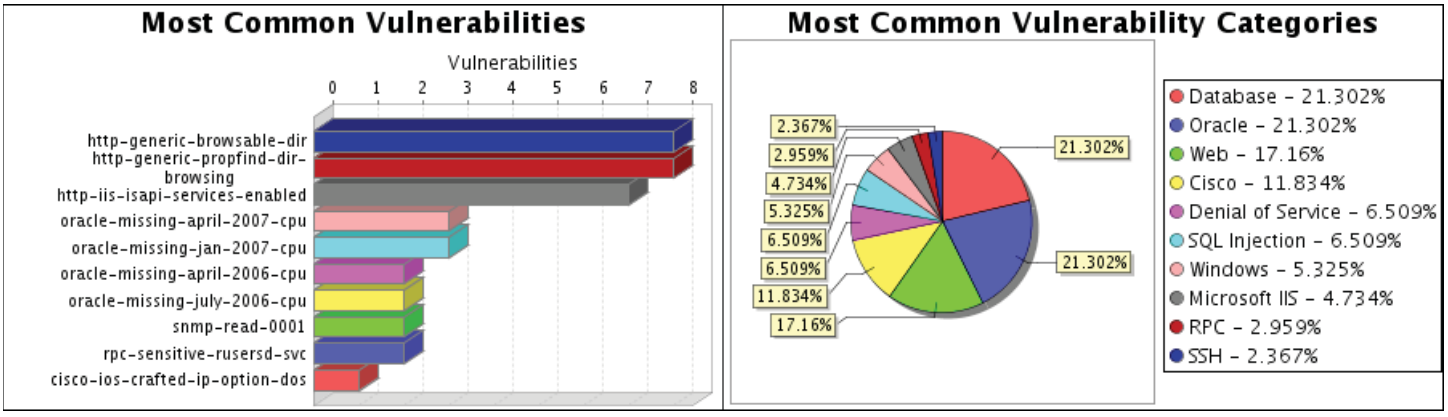
This report represents a security audit performed by NeXpose from Rapid7 LLC. It contains confidential information about the state of your network. Access to this information by unauthorized personnel may allow them to compromise your network.

Site Name	Start Time	End Time	Total Time	Status
Boston - Production	December 08, 2009 11:37, EST	December 08, 2009 11:45, EST	8 minutes	Success

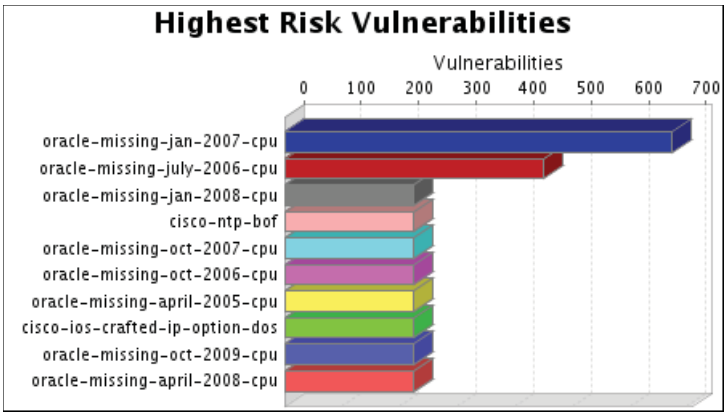
The audit was performed on 4 systems, 4 of which were found to be active and were scanned.



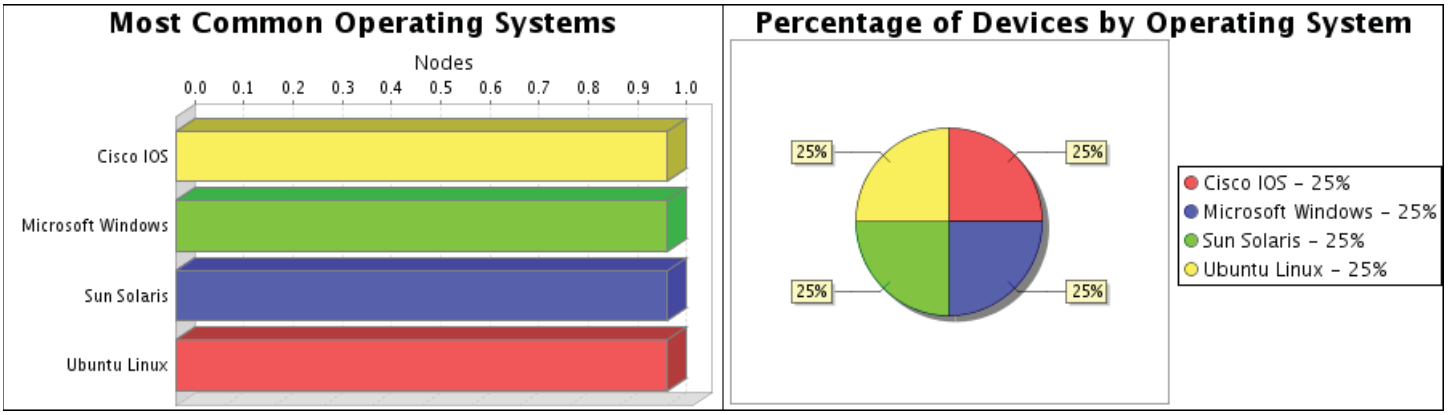
There were 107 vulnerabilities found during this scan. Of these, 34 were critical vulnerabilities. Critical vulnerabilities require immediate attention. They are relatively easy for attackers to exploit and may provide them with full control of the affected systems. 58 vulnerabilities were severe. Severe vulnerabilities are often harder to exploit and may not provide the same access to affected systems. There were 15 moderate vulnerabilities discovered. These often provide information to attackers that may assist them in mounting subsequent attacks on your network. These should also be fixed in a timely manner, but are not as urgent as the other vulnerabilities. Critical vulnerabilities were found to exist on 3 of the systems, making them most susceptible to attack. 4 systems were found to have severe vulnerabilities. Moderate vulnerabilities were found on 3 systems. No systems were free of vulnerabilities.



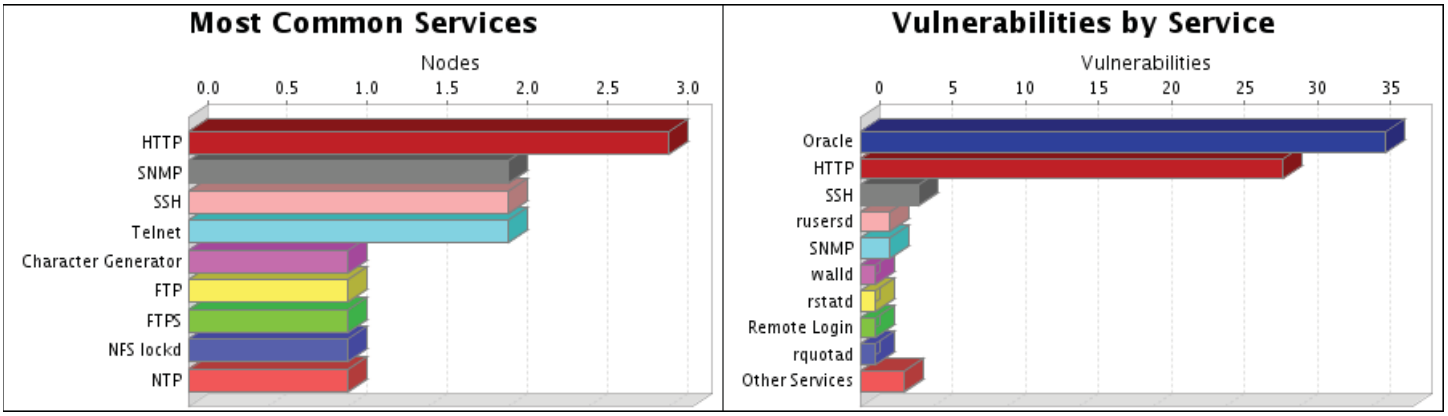
There were 8 occurrences of the http-generic-browsable-dir and http-generic-propfind-dir-browsing vulnerabilities, making them the most common vulnerabilities. There were 36 vulnerabilities in the Database and Oracle categories, making them the most common vulnerability categories.



The oracle-missing-jan-2007-cpu vulnerability poses the highest risk to the organization with a risk score of 675. Vulnerability risk scores are calculated by looking at the likelihood of attack and impact, based upon CVSS metrics. The impact and likelihood are then multiplied by the number of instances of the vulnerability to come up with the final risk score.
There were 4 operating systems identified during this scan.



The Cisco IOS, Microsoft Windows, Sun Solaris and Ubuntu Linux operating systems were found on 1 systems, making them the most common operating systems.
There were 32 services found to be running during this scan.

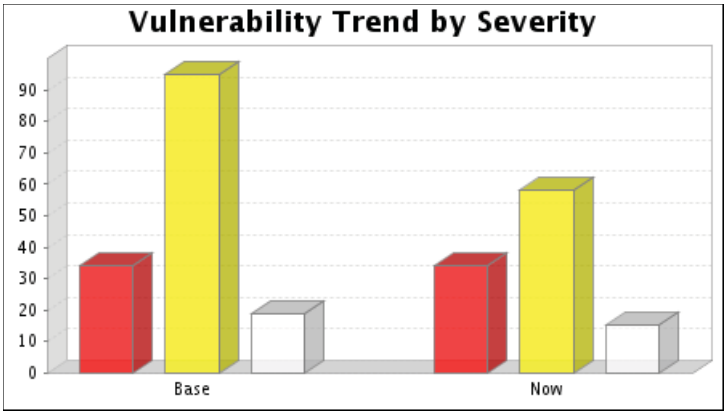


The HTTP service was found on 3 systems, making it the most common service. The Oracle service was found to have the most vulnerabilities during this scan with 36 vulnerabilities.

2. Trend Analysis

One previously discovered node was not found. No new nodes were discovered. This reduces the number of actives nodes to 4. The overall number of vulnerabilities dropped from 148 to 107. The number of critical vulnerabilities remained at 34. The number of severe vulnerabilities decreased from 95 to 58. The number of moderate vulnerabilities decreased from 19 to 15.

This represents a significant improvement in the security of the network. Having any vulnerabilities on the network is still a risk. It is important to address reported vulnerabilities as quickly as possible. Failure to do so greatly increases the risk of compromise.



The overall number of services dropped from 51 to 46. The newly discovered services were responsible for 3 vulnerabilities. Whenever adding new hardware or software, it is critical to apply all available patches. The configuration of the service should also be checked to make sure all possible security measures are in place. The previously discovered services that are no longer present were responsible for 3 vulnerabilities. This is a positive step if the services were disabled in response to those vulnerabilities.