Executive Overview

Los Angeles Exec-Overview

Audited on April 05 2010

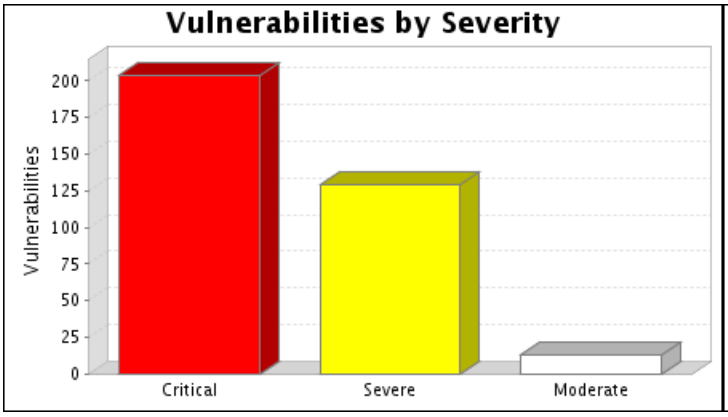
Reported on December 17 2010

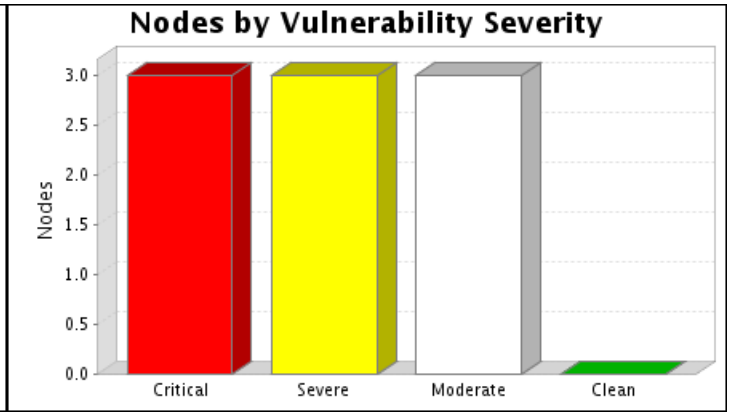
1. Executive Summary

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.

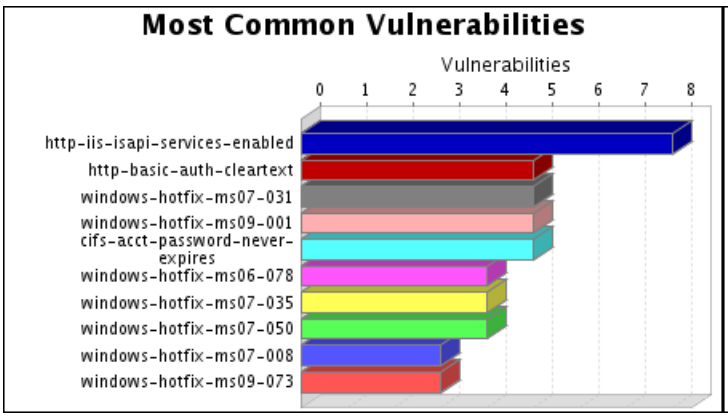
Site Name	Start Time	End Time	Total Time	Status
Los Angeles - LAN	April 05, 2010 20:00, EDT	April 05, 2010 20:05, EDT	5 minutes	Success

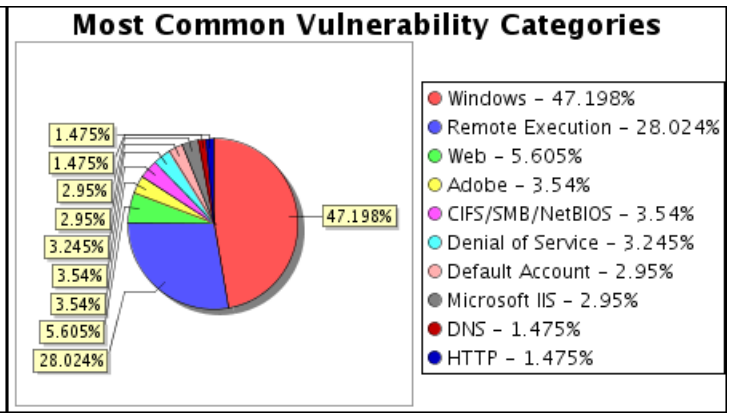
The audit was performed on 3 systems, 3 of which were found to be active and were scanned.



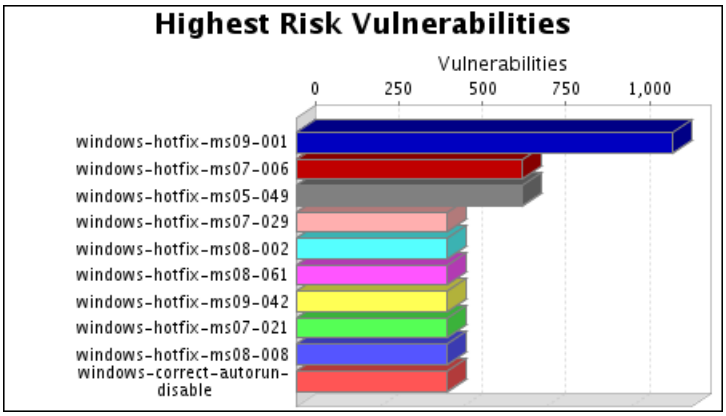


There were 346 vulnerabilities found during this scan. Of these, 204 were critical vulnerabilities. Critical vulnerabilities require immediate attention. They are relatively easy for attackers to exploit and may provide them with full control of the affected systems. 129 vulnerabilities were severe. Severe vulnerabilities are often harder to exploit and may not provide the same access to affected systems. There were 13 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. 3 systems were found to have severe vulnerabilities. Moderate vulnerabilities were found on 3 systems. No systems were free of vulnerabilities.

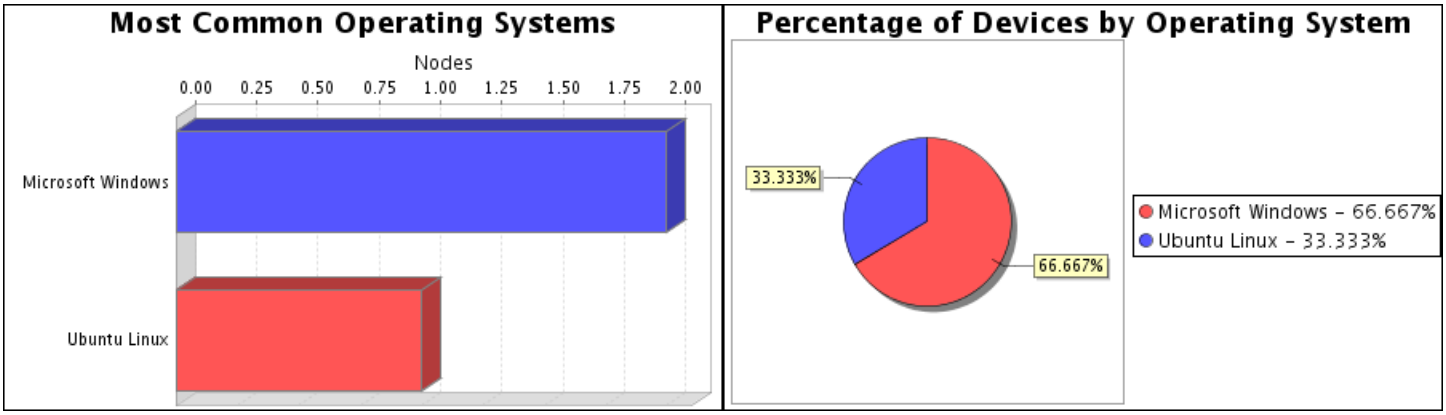




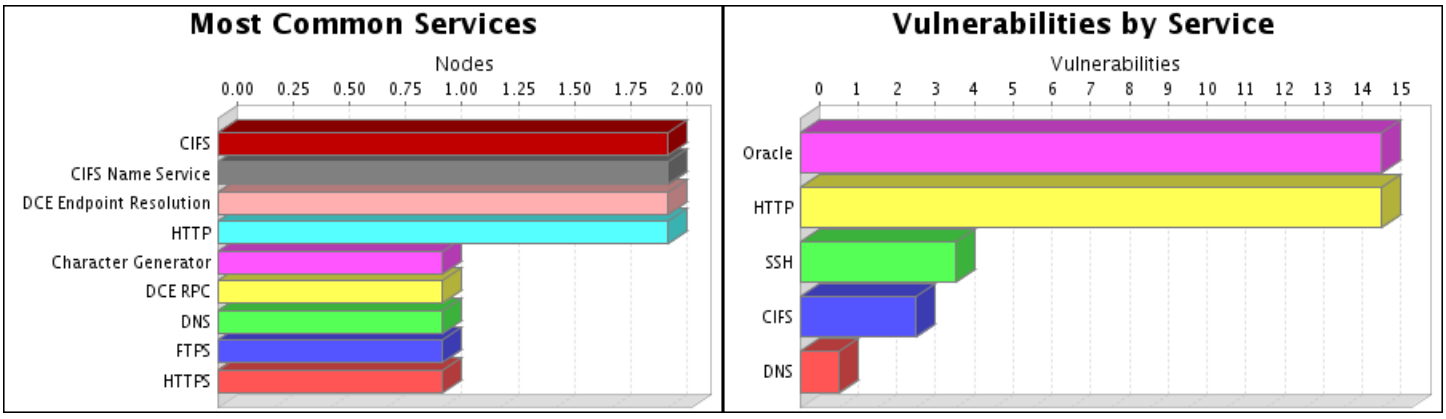
There were 8 occurrences of the http-iis-isapi-services-enabled vulnerability, making it the most common vulnerability. There were 160 vulnerabilities in the Windows category, making it the most common vulnerability category.



The windows-hotfix-ms09-001 vulnerability poses the highest risk to the organization with a risk score of 1,125. 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 2 operating systems identified during this scan.



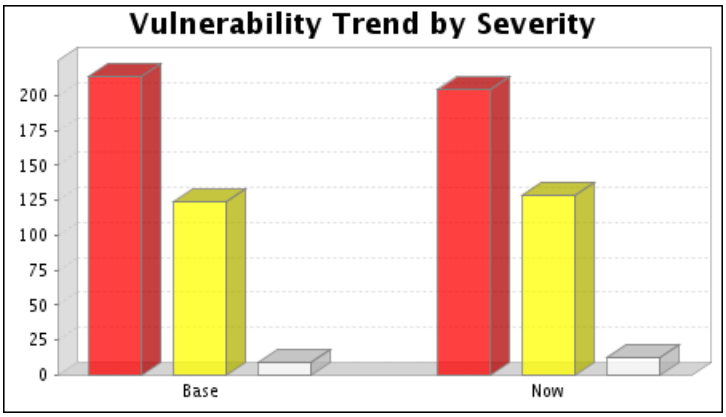
The Microsoft Windows operating system was found on 2 systems, making it the most common operating system.
There were 17 services found to be running during this scan.



The CIFS, CIFS Name Service, DCE Endpoint Resolution and HTTP services were found on 2 systems, making them the most common services. The Oracle and HTTP services were found to have the most vulnerabilities during this scan, each with 15 vulnerabilities.

2. Trend Analysis

The list of active nodes remained the same. No new nodes were discovered, and the previously discovered nodes were still active. The overall number of vulnerabilities dropped from 347 to 346. The number of critical vulnerabilities decreased from 214 to 204. The number of severe vulnerabilities increased from 124 to 129. The number of moderate vulnerabilities increased from 9 to 13.
This trend does not reflect a significant change in the security of the network. 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 36 to 35. The newly discovered services were responsible for 12 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 1 vulnerabilities. This is a positive step if the services were disabled in response to those vulnerabilities.