ENDPOINT APPLICATION DISCOVERY TOOL FOR WINDOWS

Executive Summary

Prepared for Acme Inc

Scan Date 10/08/2016 11:32:21. Scan completed in 5 minutes.

Knowing the applications installed on your network is one of the first steps to securing your endpoints. Having an inventory of operating system configurations is necessary in order to know if there are any vulnerabilities that could be mitigated by patching or removing the applications affected. Maintaining up-to-date operating systems and software helps with endpoint security. With automated tools that inventory and flag security issues, the process of knowing what is on your network is easier and helps keep networks secure.

The analysis scanned the Windows Workstations and Servers on the network for their general properties and the applications installed on them. Controlling the entire surface area of your network related to operating systems and the applications installed on them is critical to maintaining your security posture. Many times untrusted or malicious applications are installed onto machines without administrator knowledge which can compromise the network's security. The data used to find systems with vulnerable products was correlated from the NIST National Vulnerability Database and the Common Platform Enumeration.

Additionally – two other excel files were also created that include a full inventory of the systems scanned and the applications discovered. You can find them in the same folder where this report was created.

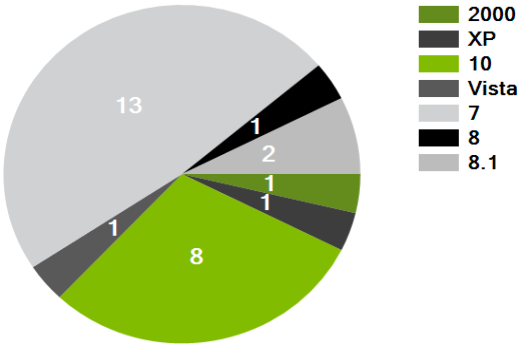
- There are many computers that have risky applications installed. The product inventory should be reviewed and locking down OS configurations should be considered.
- There are older Windows Workstation operating systems on your network. Consider upgrading Windows 2000 and XP workstations.

Executive Summary Continued

- There are vulnerable versions of known risky applications installed on network endpoints. It is important to keep these applications up-to-date if unable to uninstall them from the endpoints.

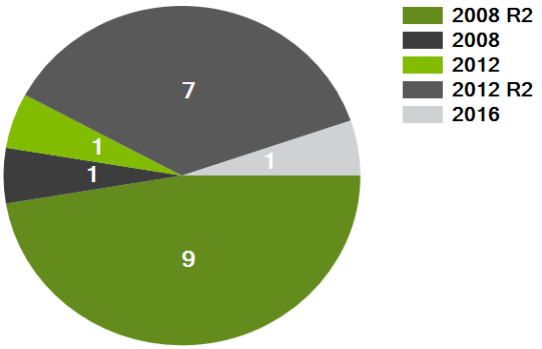
After reviewing the various reports, it is easy to see that improvements can be made to security which could greatly reduce your organization's risk to attack. Consider securing your endpoints before they become the target for attackers. Reduce the vulnerabilities on your endpoints!

Endpoint Application Discovery Tool



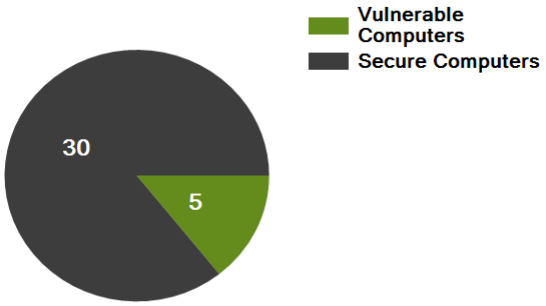
Workstation Operating System Distribution

Careful! It is important to keep Operating Systems up-to-date with their latest versions to ensure they receive the most recent security patches. Older Operating Systems could pose a security risk to the network if not secured. Windows 2000 and XP computers should be upgraded. Time to protect your systems!



Server Operating System Distribution

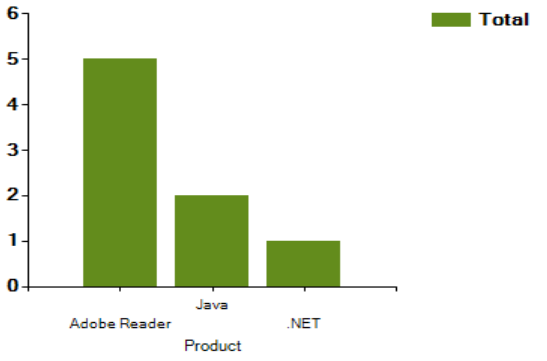
Great! All of the operating systems discovered are still being supported with security patches. It is important to keep Operating Systems up-to-date with their latest versions to ensure they receive the most recent security patches. Older Operating Systems could pose a security risk to the network if not secured. Continue monitoring your endpoints for any negative changes to your great setup!



Vulnerable Computers

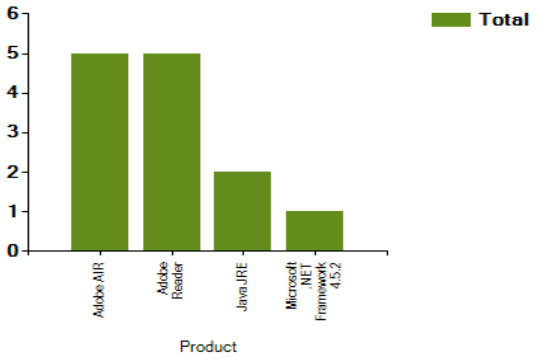
Warning! It appears your network contains one or more vulnerable computers. It is important to create OS configurations that do not have vulnerable or risky software in order to better secure your network. An application is vulnerable or risky if it has a CVE issued for a version currently installed. Time to protect your systems!

Endpoint Application Discovery Tool



Known Risky Applications

Look Out! There appears to be a number of known risky applications installed on the network. It is important to keep track of potentially risky applications in order to keep their security patches up-to-date. In some cases, it may not be feasible to remove these applications, so continuous endpoint security monitoring is necessary to know when to update. Time to protect your systems!



Top Vulnerable Applications

These are the top 5 vulnerable applications found on your endpoints. Knowing if an application you have added to an OS configuration has a vulnerability is useful for maintaining the health and security of your endpoints. Time to protect your systems!