Detection, Identification and Reporting of Software Vulnerabilities

Software Vulnerability Assessment

In computer security, a vulnerability is a weakness which allows an attacker to reduce a system's information assurance. Unfortunately, software-based vulnerabilities provide an easy way for hackers to get into your systems. It's very important to be able to recognize software vulnerabilities so you can quickly identify and report on any machines or installed software that may be a threat to your IT environment.

Network and endpoint security is no longer just the domain of corporate IT security teams. Today's security initiatives are far-reaching and often involve many different organizations and systems. Asset management teams can provide essential input to these initiatives since they have a tremendous amount of current information about installed hardware and software at their fingertips.

The Solution

Now your ITAM and SAM programs can help reduce your organization's risk with Eracent's Software Vulnerability Assessment. The valuable functionality provided by this module is based on standardized data that is continuously gathered by the National Institute of Standards and Technology (NIST). Several times a day, NIST updates their National Vulnerabilities Database (NVD) of all known exposures that exist in commercial IT hardware and software products. Within hours of the NIST database being updated, Eracent maps this new vulnerability data to product records in both the SCANMAN™ software recognition library and the IT-Pedia® IT Product Data Library.

As a result, ITMC Discovery™ can quickly identify any installed products that have known vulnerabilities. You can see any potential threats and software that needs to be patched, updated or replaced.

519 Easton Road
Riegelsville, PA 18077

+1 908.537.6520
www.eracent.com
info@eracent.com

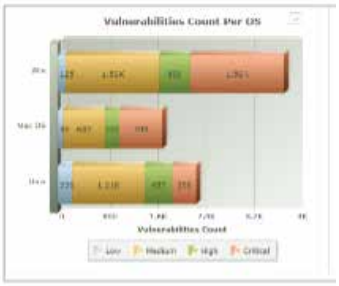
Standard reports and dashboards include:

- Vulnerabilities by individual machine, OS, publisher or product
- Makes, models, application names, versions and editions
- Applicable licensing programs and product use rights

Being able to quickly identify any machines or installed software that may be a threat is just one aspect of a broader network security initiative, but it can be a very effective piece of the puzzle.

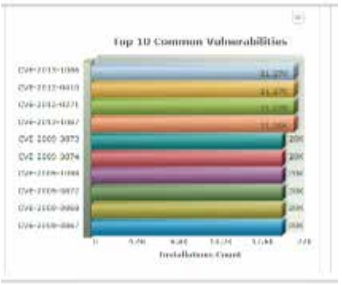
Verifying Standard Images

ITMC Discovery provides another level of protection by ensuring that your environment is fully covered from a security standpoint. Discovery scans detect the presence of any installed anti-virus software and can indicate unprotected machines. Scans can also check for all applicable Windows patches and can report on any machines that deviate from the most current, up-to-date standard image.

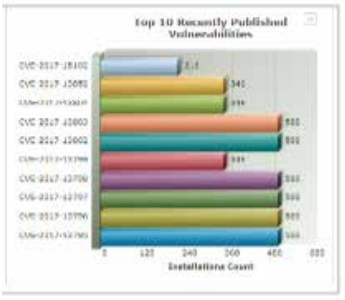


Software End-of-Life Data

Another element in preventing unwanted network intrusion is software end-of-life (EOL) and end-of-support (EOS) data. If a product or version is still installed after it reaches one of these dates, it creates a security risk since it will not be possible to get a patch or fix from the publisher. Having EOL and EOS data available makes it easier to plan for refresh cycles and avoid potential software-based threats.



Eracent continuously gathers and consolidates EOL and EOS data in IT-Pedia, and automated updates are available on a daily basis. This information can be easily shared with ITSM, ITAM, SAM and other systems via multiple integration methods.



For information on Software Vulnerability Assessment or the end-of- life and end-of-support details provided in IT-Pedia, contact your Eracent representative or inquire via info@eracent.com.

519 Easton Road, Riegelsville, PA 18077

+1 908.537.6520
www.eracent.com | info@eracent.com