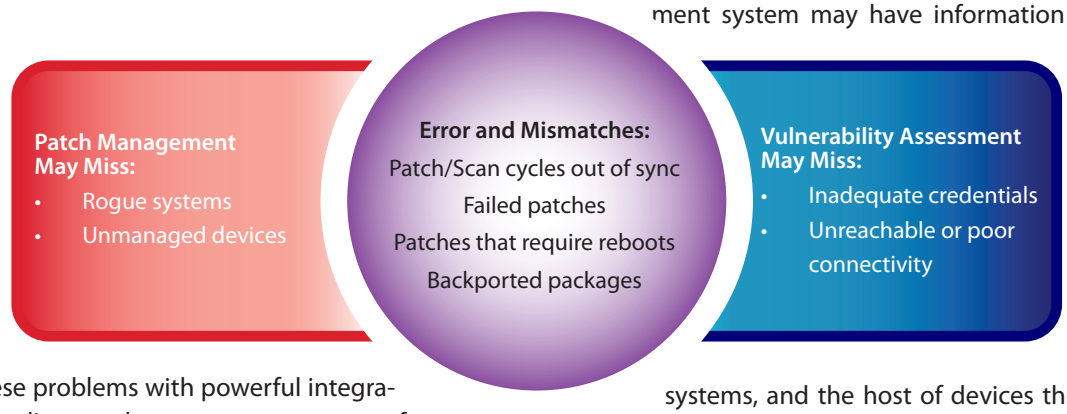
TENABLE Network Security®

The Great Divide

Bridging the Gap Between Patch Management and Vulnerability Assessment

With two distinct views of the same IT resources, it's essential patch management and vulnerability assessment systems agree on the status of the systems they control. But too often they don't– discrepancies between these critical management systems are common, with consequences that include failed compliance checks, unsatisfactory audit findings, and even increased friction between IT security and operations groups. Regardless of whether you measure the cost in frayed tempers, lost business, or fines and damaged reputations, the impact to the bottom line is real and growing.

Tenable, whose Nessus Scanner–with over five million downloads–is the industry's de facto standard for vulnerability assessment, delivers a solution to these problems with powerful integration to market leading patch management systems from Red Hat, Microsoft, and VMware.



"We have seen in increase in clients who are tying patch automation to configuration auditing for compliance. These two functions often go hand in hand because many compliance violations are actually due to unpatched systems."

Gartner Market Trends and Dynamics for Server Provisioning and Configuration Management Tools, Ronni Colville and Donna Scott, 28 March 2011 ID: G00211468

HIGH STAKES FOR IT MANAGEMENT

Discrepancies between patching and vulnerability assessment systems represent much more than an annoyance or distraction. The consequences of these systems being out of alignment are serious, and include failed regulatory compliance checks, adverse and unsatisfactory audit findings, increased risk, inefficiencies that waste valuable time and resources, and even needless friction between IT operations and security groups.

Many regulatory and industry compliance initiatives dictate periodic assessments of network resources to ensure that vulnerabilities in network resources are eliminated, and that adequate processes are in place to maintain the integrity and security of those resources.

MANAGEMENT MISMATCHES

Multiple situations can arise that lead to discrepancies between patch management and vulnerability assessment systems.

- For example, since its results are based on an actual assessment of the environment, the vulnerability assessment system may have information about resources unknown to the patch management system. These include new systems that have not yet been placed under the control of the patching system, rogue systems, and the host of devices the patch management system isn't capable of managing (network devices, printers, mobile systems, etc.).
- Similarly, the vulnerability assessment system may have an incomplete or imprecise view of the network. Scanners may have been deployed incorrectly or inadequately, leaving parts of the network out of sight. The vulnerability assessment system may lack credentials to systems being scanned, leading to inaccurate data. In some cases, a vulnerability assessment system may lack operating system or application support and thus is unable to provide an assessment of a given system.

Even when both systems are aware of a given resource, things can still go wrong that will lead to discrepancies:

- Application of a patch may fail for some reason, leading the patch management system to report it as applied while a scan of the system reveals the fix is missing.
- Some systems, particularly Windows-based operating systems, require a reboot or restart for the patch to be completely installed. Again, the patch management system will report the patch as applied, but the system isn't truly protected.

- Inaccurate or incomplete vulnerability assessments can generate false positive warnings of missing patches.
- Mismatches between scanning and patching cycles lead to confusion. If a system is scanned before it's patched, the vulnerability assessment system will continue to report the system as at risk until another vulnerability assessment is performed. Depending on the tool and the organization's policies and processes, that might mean weeks or months of false alarms.
- Back-ported patches, current fixes retroactively applied to older releases of software, can trip up vulnerability assessment systems. Discovering a back-level release of software deployed, the vulnerability assessment system reports a flaw which has actually been fixed.

AGREEING TO DISAGREE?

Discrepancies like these can lead to serious consequences, including failed regulatory compliance checks, adverse audit findings, increased risk, inefficiencies, and even friction between IT operations and security groups.

- Many regulatory and industry compliance initiatives require periodic assessments of network resources to demonstrate that processes are in place to maintain operating system and application patches, and to ensure vulnerabilities are eliminated. If a vulnerability scan generates a false positive–reporting a system is vulnerable when it actually isn't–the organization risks failure to achieve compliance. That can negatively affect the viability of the business, lead to fines and other penalties, and create extra cost and work as staff attempt to explain discrepancies and re-scan problem systems.
- Audit processes can fall prey to issues like these, with similar consequences.
- Discrepancies between patch management and vulnerability assessment have the potential to create extra cost and work for both the security team and IT operations:
    - Identifying systems at risk to an emerging vulnerability/exploit is more difficult since information isn't consistent–security teams lose confidence in data and must perform additional checks and tests.
    - Managing the patching process is more difficult under conditions of uncertainty–metrics, such as the number of days required to apply patches, systems unpatched for 30- or 90- days, and so on–are seen as unreliable and inaccurate.
    - These mismatches and misinformation inevitably lead to finger pointing and acrimony between groups and teams.

TENABLE'S SOLUTION

Tenable uniquely provides robust integration between the Nessus Scanner and popular patch management solutions including:

- Red Hat Satellite Server (bi-directional, with support for both interrogating patch management systems for the status of specific resources, and the ability to request the application of missing patches to targeted systems)
- Microsoft Windows Server Update Services (WSUS)
- Microsoft System Center Configuration Manager (SCCM)
- VMware Go

Nessus patch management integration allows Nessus to query patch management systems directly, and retrieve patch status for all relevant systems quickly and reliably, without the need to interrogate the system being managed. This capability supports:

- Fast and easy generation of patch compliance reports in Nessus and SecurityCenter, based on the data returned from patch management systems. Presentation of records in the well-known Nessus format can speed auditors' reviews, and simplifies resolution of discrepancies between management systems.
- The ability to retrieve accurate patch status information for systems that can't be fully scanned by vulnerability assessment tools because of a lack of credentials. Credentials are only required for access to the patch management system.
- Retrieve patch status in environments where scanning is not available due to other constraints, such as limited networking.
- Patch audit comparisons, with updates to the patch management system based on credentialed host scans/audits.
- In Red Hat Satellite environments, bi-directional integration allows Nessus to proactively request the application of a patch when scans reveal it to be missing from a system.

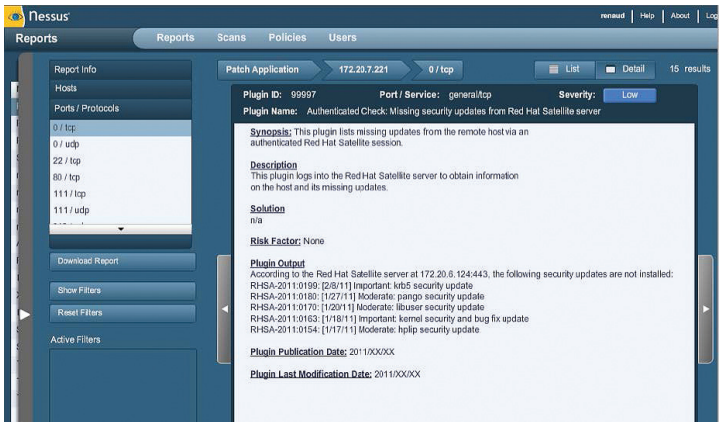


Figure 1: Nessus Patch Management integration yields highly accurate insights into the patch status of systems, increasing accuracy, improving compliance and simplifying management.

TENABLE Network Security®

ABOUT TENABLE NETWORK SECURITY

Tenable Network Security is the leader in Unified Security Monitoring. Tenable provides enterprise-class agentless solutions for the continuous monitoring of vulnerabilities, configuration weaknesses, data leakage, log management and compromise detection to help ensure FDCC, FISMA, SANS CAG and PCI compliance. Tenable's award-winning products are utilized by many Global 2000 organizations and Government agencies to proactively minimize network risk. For more information, please visit www.tenable.com.