NNT™ SECURITY THROUGH SYSTEM INTEGRITY | VULNERABILITY TRACKER™

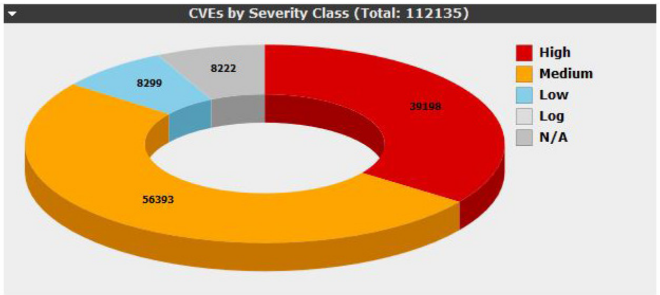
NOW PART OF netwrix

Vulnerability Tracker Solution Brief

RE-INNOVATING THE VULNERABILITY SCANNING MARKET

Through a strategic collaboration with Greenbone Networks, NNT has advanced their Security through System Integrity strategy with the adoption of distributed, fast and accurate Enterprise-class vulnerability scanning. *NNT's Vulnerability Tracker* enables organizations to cost-effectively improve their IT posture by focusing your remediation guidance on the assets that pose the highest risk to your network.

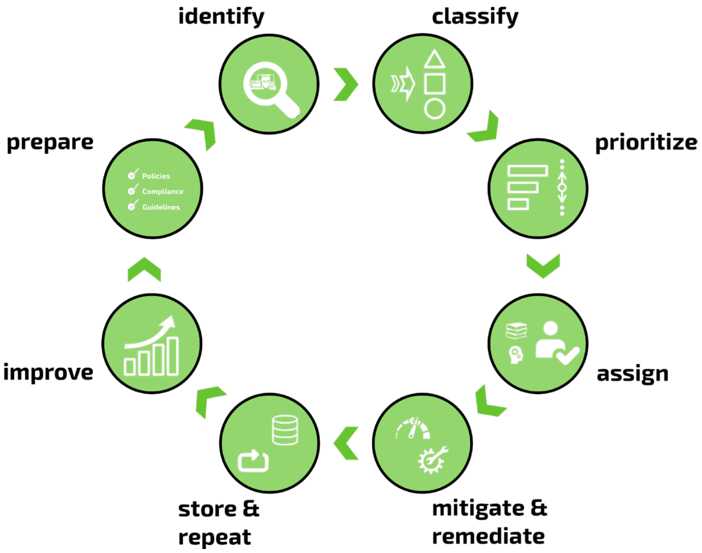
Vulnerability Tracker™ is based on the enterprise-class Greenbone version of OpenVAS, the world's most widely adopted vulnerability assessment tool. This forms a significant evolution of *NNT's SecureOps Enterprise Security Strategy* and complements NNT's award winning Change Tracker™ Gen7R2 to further efforts in solving IT Security through the definition and delivery of Integrity. Integrity is the cornerstone of any successful cybersecurity strategy and is defined by the SANS Institute and Center for Internet Security as the most critical pillar to achieving a trusted platform.



VULNERABILITY MANAGEMENT: AN ESSENTIAL CONTROL

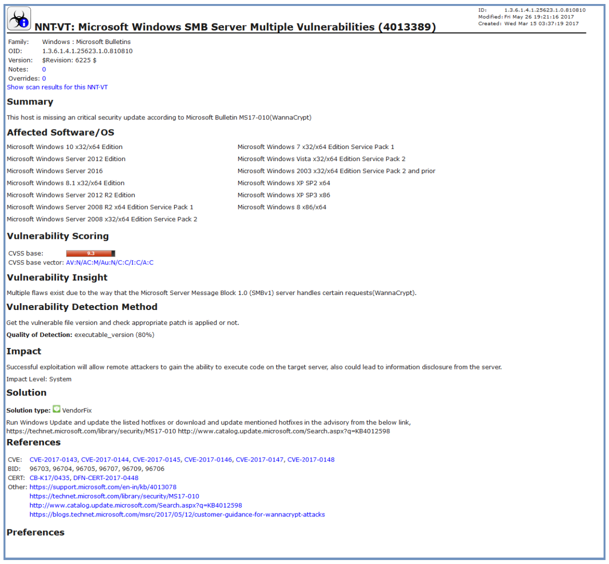
Vulnerability Scanning is a core foundational security control identified by the *Center for Internet Security's Top 20 CIS Controls*. Vulnerability Tracker™ directly addresses the CIS Controls for Inventory, Secure Configurations, Control of Ports and Services and of course, Continuous Vulnerability Assessments. As one of a handful of CIS Certified vendors, your organization can guarantee that the integrity and security of all your IT systems are hardened and free or all known vulnerabilities.

Vulnerability Tracker helps organizations significantly reduce the attack surface of an IT Infrastructure by providing an outside-in perspective, instead of inside-out. With Vulnerability Management, your goal is to identify any vulnerability that might exists within your IT infrastructure, just as a potential attacker would.



Vulnerabilities often times derive from improper configurations or programming errors, unauthorized installations, or violations of security measures, but vulnerability scans represent the first step towards detecting these misconfigurations.

Our Vulnerability Tracker solution uncovers these and other risks and helps you prioritize vulnerabilities that need to be addressed immediately before they can be exploited by a cyber attack. For any vulnerabilities identified, full details of the exploit are provided, along with clear and concise guidance to remediate and eliminate the threat.



ID: 1.3.6.1.4.1.25623.1.0.810810
Modified: Fri May 26 19:21:16 2017
Created: Wed Mar 15 03:37:19 2017

NNT-VT: Microsoft Windows SMB Server Multiple Vulnerabilities (4013389)

Family: Windows : Microsoft Bulletins
OID: 1.3.6.1.4.1.25623.1.0.810810
Version: $Revision: 6225 $
Notes: 0
Overrides: 0
Show scan results for this NNT-VT

Summary

This host is missing an critical security update according to Microsoft Bulletin MS17-010(WannaCrypt)

Affected Software/OS

Microsoft Windows 10 x32/x64 Edition
Microsoft Windows Server 2012 Edition
Microsoft Windows Server 2016
Microsoft Windows 8.1 x32/x64 Edition
Microsoft Windows Server 2012 R2 Edition
Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1
Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2
Microsoft Windows 7 x32/x64 Edition Service Pack 1
Microsoft Windows Vista x32/x64 Edition Service Pack 2
Microsoft Windows 2003 x32/x64 Edition Service Pack 2 and prior
Microsoft Windows XP SP2 x64
Microsoft Windows XP SP3 x86
Microsoft Windows 8 x86/x64

Vulnerability Scoring

CVSS base: 9.3
CVSS base vector: AV:N/AC:M/Au:N/C:C/I:C/A:C

Vulnerability Insight

Multiple flaws exist due to the way that the Microsoft Server Message Block 1.0 (SMBv1) server handles certain requests(WannaCrypt).

Vulnerability Detection Method

Get the vulnerable file version and check appropriate patch is applied or not.

Quality of Detection: executable_version (80%)

Impact

Successful exploitation will allow remote attackers to gain the ability to execute code on the target server, also could lead to information disclosure from the server.

Impact Level: System

Solution

Solution type: VendorFix

Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory from the below link,
https://technet.microsoft.com/library/security/MS17-010 http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012598

References

CVE: CVE-2017-0143, CVE-2017-0144, CVE-2017-0145, CVE-2017-0146, CVE-2017-0147, CVE-2017-0148
BID: 96703, 96704, 96705, 96707, 96709, 96706
CERT: CB-K17/0435, DFN-CERT-2017-0448
Other: https://support.microsoft.com/en-in/kb/4013078
https://technet.microsoft.com/library/security/MS17-010
http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012598
https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks

Preferences

Vulnerability Tracker Solution Brief

ELIMINATE RISK WITH VULNERABILITY TRACKER

Vulnerability Tracker allows you to stay several steps ahead of attackers – once you know where the kinks in your infrastructure lie, you can take the remediation steps necessary to stop attackers from executing a cyber-attack.

With Vulnerability Tracker, your organization is able to quickly identify and reduce the attack surface, giving you better control and assurance that your infrastructure is operating with the least amount of risk.

Today's threat landscape is constantly changing, but with Vulnerability Tracker, your organization is able to quickly identify any new vulnerabilities introduced into your network against 66,000 Network Vulnerability Tests (NVTs). New vulnerabilities are added daily through various content providers and industry resources which include over 11,400 Common Vulnerabilities and Exposure (CVEs), Bugtraq, and other trusted content providers.
CVE is the manufacturer-independent industry standard for the explicit identification and description of vulnerabilities.

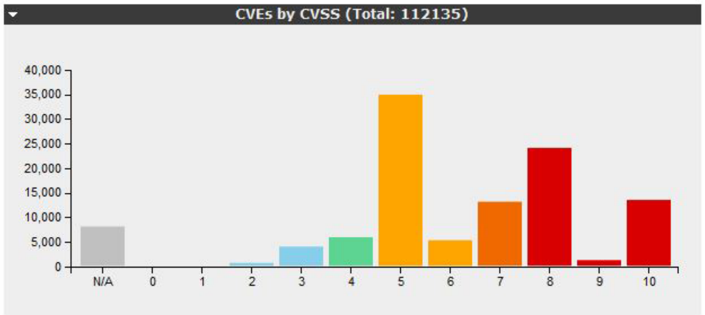
SPEED & AUTOMATION

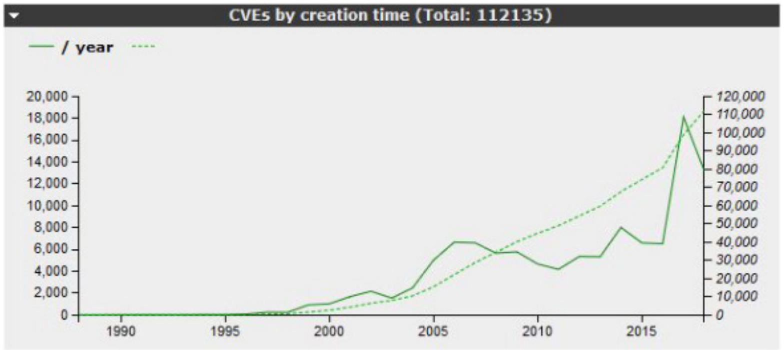
NNT Vulnerability Tracker helps organizations maximize scanning efficiency with hyper fast scanning technology and fewer false positive. Vulnerability Tracker delivers class-leading accuracy, guaranteeing the lowest false positive per scan ratio in the vulnerability scanning market. Our hyper-fast scanning technology means your organization can assess over 50,000 endpoints per 24 hours.

Vulnerability Tracker automatically transfers scan results to the management process, allowing you to see at a glance what vulnerabilities exist, if they have been addressed by your IT administration, or if any new vulnerabilities have been discovered within the ongoing vulnerability assessment.

VULNERABILITY TRACKER KEY BENEFITS:

- Turn-key solution: ready to use within 10 minutes
- Powerful appliance operating systems with special command line administration based on comprehensive security design
- Integrated Greenbone Security Feed with over 66K Network Vulnerability Tests
- Integrated Backup, Restore, Snapshot and Update
- No limitations on number of target systems or IPs
- Scan task management with false positive marking
- Choice between blended credentialed and non-creden tialed tests





About NNT

New Net Technologies (NNT) is the leading provider of Secure Ops, which leverages security through System Integrity along with Intelligent Closed Loop Change Control, focused on helping organizations reduce their security risk, increase service availability and achieve continuous compliance. NNT delivers its Secure Ops suite by combin-ing: System Configuration Hardening, Closed Loop Change Control, Vulnerability Management and Event Log Management. These core security disciplines are defined by the SANS Institute as the essential Critical Security Controls for any cyber security initiative. W: www.newnettechnologies.com E: info@nntws.com