VSA-7

ANALIZADOR DE VULNERABILIDADES

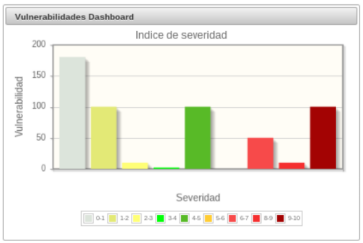
La seguridad informática de los sistemas de operación es un factor muy relevante debido a su impacto directo sobre la disponibilidad y la confiabilidad de los mismos. Conseguir una protección informática que garantice el objetivo de desempeño de nuestro sistema optimizando los costes es muy complejo si no disponemos de datos fiables y detallados del entorno del sistema.
Conocer las vulnerabilidades de nuestro sistema es el primer paso para implementar una protección eficaz.
Un reporte detallado de vulnerabilidades permite una configuración optimizada de las medidas de protección y contribuye a que el diseño del sistema sea intrínsecamente seguro.

VENTAJAS

Análisis no intrusivo. Durante el proceso de análisis, el equipo inspeccionado puede seguir funcionando de forma normal.

Resultados normalizados. La aplicación VSA-7 utiliza el método de cálculo de la severidad de las vulnerabilidades (CVSS) definido por el foro FIRST.

Perfil de análisis personalizado. La herramienta VSA-7 utiliza un perfil de análisis personalizado para las vulnerabilidades que pueden afectar a los sistemas de operación. De esta forma se agiliza el proceso de análisis y los resultados son de aplicación directa.



Formato Reporte

High (CVSS: 9.3)
NVT: Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)

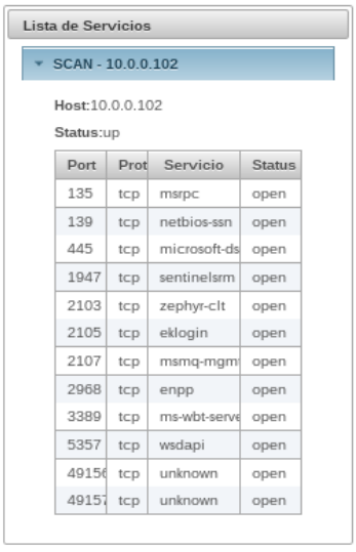
Summary
This host is missing a critical security update according to Microsoft Bulletin MS17-010.

Vulnerability Detection Result
Vulnerability was detected according to the Vulnerability Detection Method.

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

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 7 x32/x64 Edition Service Pack 1 Microsoft Windows Vista x32/x64 Edition Service Pack 2 Microsoft Windows Server 2008 R2 x64 Edition Service Pack 1 Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2



ARTEC INGENIERIA

PULLNET Telecom for energy

FUNCIONALIDADES

VSA-7

Análisis de servicios.

Muestra los servicios activos en el dispositivo que está siendo analizado. Indica el nombre y tipo de servicio, el puerto utilizado y el estado. Esta información es muy útil para identificar servicios innecesarios para la funcionalidad implementada por dicho equipo los cuales pueden facilitar ataques informáticos y en consecuencia deberían ser desactivados.

Identificación de vulnerabilidades

Identifica las vulnerabilidades del equipo o sistema analizado indicando sus características

- Nivel de severidad. Calculado utilizando la normativa mediante la cual se obtiene el nivel de severidad o CVSS
- Identificación oficial o código CVE
- Descripción de la vulnerabilidad
- Posibles vectores de ataque
- Remedios si se conocen

Interfaz de usuario en tiempo real

El interfaz de usuario presenta en tiempo real las vulnerabilidades identificadas. El usuario puede detener la prueba en todo momento

Reportes de resultados

La aplicación VSA-7 genera de forma automática reportes de los resultados de los análisis de vulnerabilidades en formato pdf. Dichos reportes pueden incluir resultados de un equipo o de un sistema formado por varios equipos. En ambos casos, los reportes quedan firmados con una firma digital de forma que se puede validar su autenticidad.

Precisión del análisis

La aplicación VSA-7 indica el grado de certeza de la detección de cada vulnerabilidad. Este valor se presenta en porcentaje para cada una de las vulnerabilidades detectadas. Si el porcentaje de precisión es bajo debería considerarse la realización de otros tipos de pruebas.

ESPECIFICACIONES TÉCNICAS

Requerimientos de Hardware

- Procesador Intel® DualCore® o superior
- 8GB de RAM
- 512 GB de disco duro
- Interface Ethernet 10/100/1000 BaseT
- Interfaz USB opcional

Requerimientos de Sistema Operativo

- Compilación específica de Linux incluida en el instalable

LICENCIAS

- Temporales por 3, 6 o 12 meses
- Permanentes
- Licencia para análisis de un solo host
- Licencia para análisis simultáneo de múltiples hosts

ARTEC INGENIERIA

PULLNET Telecom for energy