

VM

VULNERABILITY MANAGEMENT

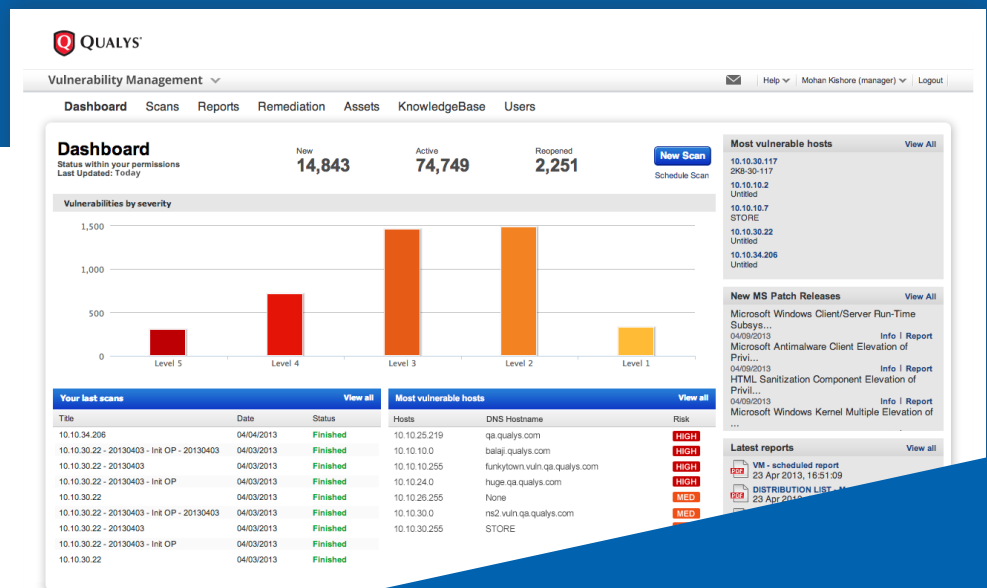
Detecte e proteja-se continuamente contra ataques sempre que eles surgirem e onde quer que seja

Tudo que você precisa para ter segurança e conformidade contínuas

Adquira o Qualys VM como um aplicativo independente ou como parte da plataforma de nuvem da Qualys. É uma plataforma de segurança e conformidade em que é possível detectar, defender e proteger todos os seus ativos globais de TI onde quer que eles estejam.

O Qualys Security and Compliance Suite inclui as valiosas ferramentas a seguir:

- AV** – AssetView
- CM** – Continuous Monitoring
- VM** – Vulnerability Management
- PC** – Policy Compliance
- SAQ** – Security Assessment Questionnaire
- PCI** – PCI Compliance
- WAS** – Web App Scanning
- WAF** – Web App Firewall
- MD** – Malware Detection
- SEAL** – Qualys Secure Seal



O Qualys Vulnerability Management (VM) é um serviço em nuvem que proporciona visibilidade global imediata de onde seus sistemas de TI podem estar vulneráveis às mais novas ameaças da Internet e como protegê-los. Ele ajuda você a identificar continuamente as ameaças e a monitorar mudanças inesperadas em sua rede antes que elas se tornem violações.

Baseado na principal plataforma em nuvem de segurança e conformidade do mundo, o Qualys VM mantém você livre dos problemas de custos altos, implementação e recursos associados aos produtos de software tradicionais. Conhecido por sua rápida implementação, precisão e escalabilidade incomparáveis, bem como sua avançada integração com outros sistemas corporativos, o Qualys VM é usado por milhares de organizações pelo mundo.



Benefícios:

Solução dimensionável para proporcionar cobertura de segurança abrangente de todas as redes e dispositivos.

Baixo impacto na equipe de TI para implementação, gerenciamento e uso para análise e correção.

Resultados priorizados e precisos.

O monitoramento contínuo melhora a visibilidade e a correção de vulnerabilidades para reduzir a posição de risco de sua organização.

Menor custo para garantir a segurança e a conformidade.



Recursos:

O Qualys VM é a solução mais avançada, dimensionável e extensível do setor para gerenciamento contínuo de vulnerabilidades e conformidade. Seus recursos são habilitados pela plataforma de nuvem da Qualys.

- **Dimensiona-se globalmente** sob demanda e é implementado a partir de uma nuvem privada ou pública totalmente gerenciada pela Qualys.
- **Realiza análise continuamente, identifica vulnerabilidades com precisão, prioriza essas vulnerabilidades e ajuda você a proteger** os ativos de TI no local, em locais remotos ou em dispositivos móveis, bem como em ambientes flexíveis de nuvem EC2 e Azure.
- **O painel de controle executivo** fornece um resumo da posição de segurança geral e acesso instantâneo a detalhes sobre correção.
- Como uma **solução em nuvem**, o Qualys VM está sempre atualizado.
- **Integra-se** a outros sistemas por meio das interfaces de programação de aplicativos (APIs, Application Programming Interfaces) da Qualys.
- **A criptografia completa** e os rígidos controles de acesso baseado em função mantêm seus dados de segurança em segredo.
- **Gerencia centralmente os log-ins de usuários** com Single Sign On corporativo baseado em linguagem de marcação de asserção de segurança (SAML, Security Assertion Markup Language).
- **A geração de relatórios abrangente e flexível** proporciona visibilidade da segurança com base em função, inclusive com a documentação automática de segurança para os auditores de conformidade.

Scan Results

File View Help

64.38.106.243 (2k-ep4-oe501, 2K-SPA-OE501) Windows 2000 Service Pack 3-4

Vulnerabilities (42)

- Microsoft Windows DCOM RPC Interface Buffer Overrun Vulnerability (MS03-026)
- Microsoft Windows DCOM RPCSS Service Vulnerabilities (MS03-039)
- Multiple Microsoft Windows RPC/DCOM Vulnerabilities (MS04-012)
- Microsoft Messenger Service Buffer Overrun Vulnerability (MS03-043)
- Microsoft Windows ASN.1 Library Integer Handling Vulnerability (MS04-007)
- Multiple Microsoft Windows Vulnerabilities (MS04-011)
- Windows Plug and Play Remote Code Execution (MS05-039)
- Microsoft MSDTC and COM+ Remote Code Execution Vulnerability (MS05-051)
- Microsoft Plug and Play Remote Code Execution and Local Privilege Elevation Vulnerability (MS05-047)

Details for CVE-2005-2120:

QID:	90278	CVSS Base:	6.5
Category:	Windows	CVSS Temporal:	5.1
CVE ID:	CVE-2005-2120		
Vendor Reference:	MS05-047		
Bugtraq ID:	-		
Service Modified:	06/16/2009		
User Modified:	-		
Edited:	No		
PCI Vuln:	Yes		
Ticket State:	-		

THREAT:
Plug and Play includes remote code execution and local elevation of privilege vulnerabilities. These issues could allow an authenticated attacker to take complete control of the affected system. Windows XP Embedded Systems - For additional information regarding security updates for embedded systems, refer to the following MSDN blogs: [October Security Updates are \(finally\) available](#) (KB905748)

IMPACT:
As a result of this vulnerability being exploited, an authenticated attacker could take complete control of the affected system.

SOLUTION:
Patch:
Following are links for downloading patches to fix the vulnerabilities:
[MS05-047: Microsoft Windows 2000 Service Pack 4](#)
[MS05-047: Microsoft Windows XP Service Pack 1 and Microsoft Windows XP Service Pack 2](#)

COMPLIANCE:
Not Applicable

EXPLOITABILITY:

- Core Security**
 - Reference: CVE-2005-2120
 - Description: MSRPC UMPNP/AGR MS05-047 DoS - Core Security Category: Denial of Service/Remote
- Metasploit**
 - Reference: CVE-2005-2120
 - Description: Microsoft Plug and Play Service Registry Overflow - Metasploit Ref: /modules/auxiliary/dos/windows/smb/ms05_047_znp
 - Link: http://www.metasploit.com/modules/auxiliary/dos/windows/smb/ms05_047_znp
- The Exploit-DB**
 - Reference: CVE-2005-2120
 - Description: Microsoft Windows Plug-and-Play (Umpnpmgr.dll) DoS Exploit (MS05-047) (2) - The Exploit-DB Ref.: 1271
 - Link: <http://www.exploit-db.com/exploits/1271>

ASSOCIATED MALWARE:
There is no malware information for this vulnerability.

RESULTS:
Found through SMB Transact.

- Microsoft Windows Server Service Could Allow Remote Code Execution (MS08-067)
- Microsoft SMB Remote Code Execution Vulnerability (MS09-001)
- Microsoft Windows Remote Desktop Protocol Remote Code Execution Vulnerability (MS12-020)
- EOL/Obsolete Operating System: Microsoft Windows 2000 Detected
- EOL/Obsolete Software: Microsoft Internet Information Services (IIS) 5.x Detected
- Remote User List Disclosure Using NetBIOS
- NtLm Session/Password NetBIOS Access
- Microsoft Windows Task Scheduler Code Execution (MS04-022)

Principais recursos:

Detectar

O Qualys VM detecta dispositivos novos ou esquecidos e usa a marcação dinâmica para organizar seus ativos de host por função para os negócios.

- Resultados priorizados e precisos.
- Mapeia visualmente todos os dispositivos e aplicativos na rede.
- Detalha todos os dispositivos por sistema operacional, portas, serviços e certificados.
- Monitora tudo continuamente para que você esteja no controle da segurança.

Corrigir

Monitora vulnerabilidades e o processo de correção delas. O Qualys VM controla tudo para que sua equipe possa trabalhar de modo eficiente e permanecer no controle.

- Atribui automaticamente tíquetes de correção e gerencia exceções.
- Fornece listas de patches de acordo com a prioridade de cada host e gerencia exceções.
- Integra-se a sistemas existentes de tíquetes de TI.

Avaliar

O Qualys VM analisa vulnerabilidades com precisão e eficiência em todos os lugares.

- A análise fornece resultados priorizados e precisos.
- Inclui dispositivos e aplicativos no perímetro e nas redes internas, bem como em redes de nuvem flexíveis.
- A análise é sob demanda ou agendada, até mesmo continuamente para que você seja informado sobre as mais recentes ameaças.

Informar

Relatórios abrangentes personalizados e baseados em função documentam o progresso para o departamento de TI, executivos de negócios e auditores.

- Permite emitir relatórios a qualquer momento e em qualquer lugar, sem a necessidade de uma nova análise.
- Fornece contexto e visão, não só o envio excessivo de dados.
- Mostra o progresso contínuo com suas metas de gerenciamento de vulnerabilidades.
- As APIs baseadas em XML integram dados de relatórios a GRC, SIEM, ERM, IDS e outros sistemas de segurança e conformidade.

Priorizar

Identifique os maiores riscos para os negócios usando análise de tendências, zero-day e previsões de impacto de patches. Nossa base de conhecimento contextualiza os problemas críticos. O Qualys VM ajuda a identificar tendências, ver o que mudou e prever com precisão quais hosts estão em risco, até mesmo para ataques zero-day.

Para obter uma versão de avaliação gratuita do Qualys VM válida por sete dias, acesse qualys.com/freetrial

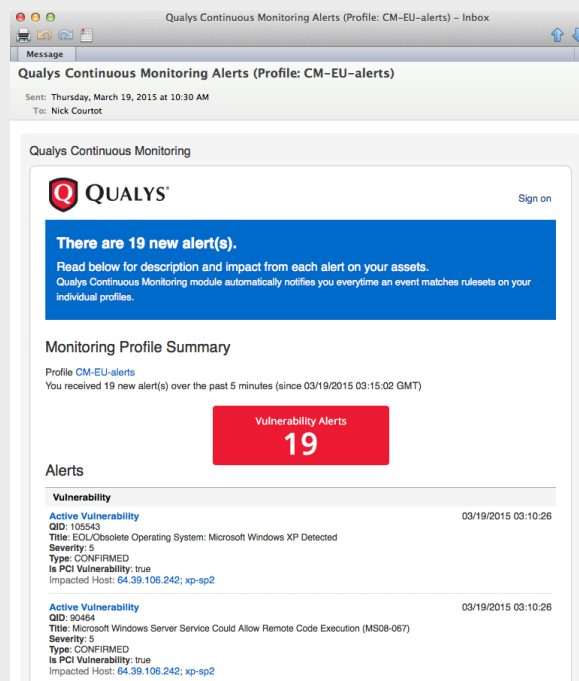
Não há nada para instalar nem fazer a manutenção

Estenda o gerenciamento de vulnerabilidades com alertas:

Monitoramento contínuo

Os alertas destinados a partir do monitoramento contínuo são imediatamente direcionados à equipe apropriada para gerar respostas mais rápidas. Isso evita que suas equipes sofram com atrasos por terem de aguardar as janelas de análises agendadas e procurar informações em longos relatórios. O recurso de monitoramento contínuo identifica imediatamente e proativamente problemas críticos de segurança, como:

- Sistemas operacionais/hosts inesperados.
- Certificados SSL prestes a expirar.
- Serviços e portas abertos inadvertidamente.
- Graves vulnerabilidades em hosts ou aplicativos.
- Software indesejado nos sistemas do perímetro.



Sobre a Qualys

A Qualys, Inc. (NASDAQ: QLYS) é pioneira e principal provedora de soluções de segurança em nuvem e conformidade com mais de 8.800 clientes em mais de 100 países, sendo que a maioria deles figuram na Forbes Global 100 e na Fortune 100. As soluções da Qualys ajudam as organizações a simplificar as operações de segurança e reduzir o custo da conformidade oferecendo inteligência de segurança crítica sob demanda e automatizando o espectro completo de auditorias, conformidade e proteção para sistemas de TI e aplicativos web. Fundada em 1999, a Qualys estabeleceu parcerias estratégicas com os principais provedores de serviços gerenciados e organizações de consultoria. A Qualys é membro fundador da Cloud Security Alliance. Para obter mais informações, acesse www.qualys.com.



Qualys, Inc. – sede
 1600 Bridge Parkway
 Redwood Shores, CA 94065 USA
 T: 1 (800) 745 4355, info@qualys.com

A Qualys é uma empresa com escritórios pelo mundo. Para encontrar um escritório perto de você, acesse <http://www.qualys.com>