QUALYS
SECURITY ON-DEMAND

ADVISORY

Qualys Security Advisory \ March 09, 2004

Microsoft Vulnerabilities: Windows Media Services, MSN Messenger, and Outlook

ADVISORY OVERVIEW

March 09, 2004 – Qualys™ Vulnerability R&D Lab has released new vulnerability signatures in the QualysGuard® Web Service to protect organizations against new Microsoft® Windows™ vulnerabilities that were announced earlier today. Customers can immediately audit their networks for these and other new vulnerabilities by accessing their QualysGuard subscription.

VULNERABILITY DETAILS

Microsoft's March 2004 Security Bulletin announced the existence of multiple new vulnerabilities affecting multiple versions of Microsoft Windows. These vulnerabilities could potentially allow an attacker to execute malicious code on a vulnerable host.

These new vulnerabilities include:

1. A vulnerability in Microsoft® Media Services 4.1 which was discovered by Qualys Vulnerability R&D Lab, described in Microsoft Security Bulletin MS04-008 (CAN-2003-0905). This vulnerability could allow a remote attacker to crash the service by sending a specially crafted packet to the Windows Media Station Service or Windows Media Monitor Service on a Windows 2000 Server. Microsoft has rated this vulnerability Moderate and recommends that users patch their servers at the earliest opportunity.
   http://www.microsoft.com/technet/security/bulletin/MS04-008.mspx

2. A vulnerability in Microsoft® Outlook 2002 and Office XP, described in Microsoft Security Bulletin MS04-009 (CAN-2004-0121). This vulnerability could allow an attacker to execute script code in the Local Machine zone on an affected system through Internet Explorer. In addition, an attacker could also create an HTML e-mail message designed to exploit the vulnerability. The attacker could then access files or execute arbitrary code on the affected system. Microsoft has rated this vulnerability Important and recommends that users patch Outlook at the earliest opportunity.
   http://www.microsoft.com/technet/security/bulletin/MS04-009.mspx

3. A vulnerability in Microsoft® MSN Messenger, described in Microsoft Security Bulletin MS04-010 (CAN-2004-0122). An attacker could send a specially crafted packet to a MSN Messenger user which would allow the attacker to view the contents of any file on the hard drive as long as the path and file name are known. Microsoft has rated this vulnerability Moderate and recommends that users patch MSN Messenger at the earliest opportunity.
   http://www.microsoft.com/technet/security/bulletin/MS04-010.mspx

HOW TO PROTECT YOUR NETWORK

Audits for the Microsoft March 2004 Security Bulletin vulnerabilities are already available in the QualysGuard vulnerability management platform. A default scan will detect these issues. In addition QualysGuard users can perform a selective scan for these specific vulnerabilities using the following checks:

- "Microsoft Windows Media Services Remote Denial of Service Vulnerability"
  - Qualys ID: 90105
  - Limit the scan to TCP ports 139, 445 and 7007
  - A Windows login is not required, but using one will provide an added level of detection.
  - Additionally, enable the "Windows Host Name" signature with Qualys ID 82044 if you want to report on vulnerable hosts by Windows (NetBIOS) machine name.

- "Microsoft Outlook Mailto Arbitrary Code Execution Vulnerability"
  - Qualys ID: 105010
  - Limit the scan to TCP ports 139 and 445
  - Windows login required
  - Additionally, enable the "Windows Host Name" signature with Qualys ID 82044 if you want to report on infected hosts by Windows (NetBIOS) machine name.

- "MSN Messenger 6 Allows Information Disclosure"
  - Qualys ID: 90106
  - Limit the scan to TCP ports 139 and 445
  - Windows login required
  - Additionally, enable the "Windows Host Name" signature with Qualys ID 82044 if you want to report on vulnerable hosts by Windows (NetBIOS) machine name.

TECHNICAL SUPPORT

For more information, customers can contact Qualys Technical Support directly at support@qualys.com or 1-866-801-6161.

Complete information about using QualysGuard's Windows Authentication feature is available in the on-line help. To access the information click Help, Network Analysis (Scans) then Windows Authentication.

ABOUT QUALYSGUARD

QualysGuard is an on-demand security audit service delivered over the web that enables organizations to effectively manage their vulnerabilities and maintain control over their network security with centralized reports, verified remedies, and full remediation workflow capabilities with trouble tickets. QualysGuard provides comprehensive reports on vulnerabilities including severity levels, time to fix estimates and impact on business, plus trend analysis on security issues. By continuously and proactively monitoring all network access points, QualysGuard dramatically reduces security managers' time researching, scanning and fixing network exposures and enables companies to eliminate network vulnerabilities before they can be exploited.

Access for QualysGuard customers: https://qualysguard.qualys.com

Free trial of QualysGuard service: http://www.qualys.com/forms/maintrial.html