QUALYS
SECURITY ON-DEMAND

ADVISORY

Qualys Security Advisory \ January 13, 2004

Multiple Microsoft Vulnerabilities

ADVISORY OVERVIEW

January 13, 2004 – Qualys™ Vulnerability R&D Lab today released new vulnerability signatures in the QualysGuard® Web Service to protect enterprises against new Microsoft® Windows™ vulnerabilities that were announced today. Customers can immediately audit their networks for these and other new vulnerabilities by accessing their QualysGuard subscription.

VULNERABILITY DETAILS

Microsoft's January Security Bulletins announced the existence of three new vulnerabilities affecting multiple versions of Microsoft Windows. These vulnerabilities could potentially allow an attacker to execute malicious code or elevate their privileges on a vulnerable host.

These new vulnerabilities are:

1. MS04-001 is a Critical-rated buffer overflow vulnerability in the Microsoft Firewall Service component of the Microsoft® ISA Server™ 2000 (CAN-2003-0819) that could allow a remote attacker to execute malicious code. For additional information about affected Microsoft platforms and available patches, please visit the Microsoft Security Bulletin at:
   http://www.microsoft.com/technet/security/bulletin/ms04-001.asp

2. MS04-002 is an NTLM authentication vulnerability in Microsoft® Outlook® Web Access for Windows Exchange Server that could allow an attacker to escalate their privileges under certain conditions. For additional information about this vulnerability, please visit the Microsoft Security Bulletin at:
   http://www.microsoft.com/technet/treeview/?url=/technet/security/bulletin/MS04-002.asp

3. MS04-003 is a buffer overflow vulnerability in Microsoft Data Access Components (MDAC) could allow a remote attacker to execute malicious code.
   http://www.microsoft.com/technet/treeview/?url=/technet/security/bulletin/MS04-003.asp

HOW TO PROTECT YOUR NETWORK

Checks for the Microsoft January 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 Internet Security and Acceleration Server 2000 H.323 Filter Buffer Overflow Vulnerability" (CAN-2003-0819) (MS04-001)
  - Qualys ID: 90088
  - Limit the scan to TCP ports 139 and 445
  - Windows login required

- "Microsoft Exchange Server 2003 Outlook Web Access Random Mailbox Access Vulnerability" (CAN-2003-0904) (MS04-002)
  - Qualys ID: 50088
  - Limit the scan to TCP ports 25, 139 and 445
  - Windows login required

- "Microsoft MDAC Function Broadcast Response Buffer Overrun Vulnerability" (CAN-2003-0903) (MS04-003)
  - Qualys ID: 90089
  - Limit the scan to TCP ports 139 and 445
  - Windows login required

TECHNICAL SUPPORT

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

Additional information about using QualysGuard's Windows Authentication feature is available in the document "Using Windows Authentication at the Domain Level." To obtain this document, please visit the Tips & Techniques section of the Resources tab on your QualysGuard Home page.

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