QUALYS
SECURITY ON-DEMAND

ADVISORY

Qualys Security Advisory \ April 13, 2004

Microsoft Vulnerabilities: Windows, RPC/DCOM, Outlook Express and JET Database Engine

ADVISORY OVERVIEW

April 13, 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 April 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. Multiple vulnerabilities in Microsoft® Windows, described in Microsoft Security Bulletin MS04-0011 (CAN-2003-0533, CAN-2003-0663, CAN-2003-0719, CAN-2003-0806, CAN-2003-0906, CAN-2003-0907, CAN-2003-0908, CAN-2003-0909, CAN-2003-0910, CAN-2004-0117, CAN-2004-0118, CAN-2004-0119, CAN-2004-0120, CAN-2004-0123). These vulnerabilities could allow an attacker, who successfully exploited the most severe of these vulnerabilities, to take complete control of the affected system. An attacker could then take any action on the affected system, including installing programs; viewing, changing, or deleting data; or creating new accounts that have full privileges. Microsoft has rated this vulnerability Critical and recommends that users update their systems immediately. http://www.microsoft.com/technet/security/bulletin/MS04-011.mspx

2. Vulnerabilities in Microsoft® RPC/DCOM, described in Microsoft Security Bulletin MS04-012 (CAN-2003-0813, CAN-2004-0116, CAN-2003-0807, CAN-2004-0124). These vulnerabilities could allow an attacker who successfully exploited the most severe of these vulnerabilities to take complete control of the affected system. An

attacker could then take any action on the affected system, including installing programs; viewing, changing, or deleting data; or creating new accounts that have full privileges. Microsoft has rated this vulnerability Critical and recommends that users update their systems immediately.
http://www.microsoft.com/technet/security/bulletin/MS04-012.mspx

3. A vulnerability in Microsoft® Outlook Express, described in Microsoft Security Bulletin MS04-013 (CAN-2004-0380). An attacker who successfully exploited this vulnerability gains access to files and can take complete control of the affected system. Microsoft has rated this vulnerability critical and recommends that users should update their systems immediately.
http://www.microsoft.com/technet/security/bulletin/MS04-013.mspx

4. A vulnerability in Microsoft® Jet Database Engine, described in Microsoft Security Bulletin MS04-014 (CAN-2004-0197). An attacker who successfully exploits this vulnerability could take complete control of an affected system, including installing programs; viewing, changing, or deleting data; or creating new accounts that have full privileges. Microsoft has rated this vulnerability important and recommends that users should install the update at the earliest opportunity.
http://www.microsoft.com/technet/security/bulletin/MS04-014.mspx

HOW TO PROTECT YOUR NETWORK

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

- "Multiple Microsoft Windows Vulnerabilities (MS04-011)"
  - Qualys ID: 90108
  - Limit the scan to TCP ports 25, 80, 135, 139, 443, 445 and 593
  - 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.

- "Multiple Microsoft Windows RPC/DCOM Vulnerabilities (MS04-012)"
  - Qualys ID: 68528 (Upgrades and Replaces existing QID 68525)
  - Limit the scan to TCP ports 80, 135, 139, 443, 445 and 593
  - 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 Express Cumulative Security Update (MS04-013) Not Installed"
  - Qualys ID: 90110
  - 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.

- “Microsoft Jet Database Engine Buffer Overflow Vulnerability”
  - Qualys ID: 19089
  - 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