



Qualys Security Advisory \ August 13, 2003

Microsoft RPC DCOM Vulnerability

ADVISORY OVERVIEW

August 13, 2003 – Qualys™ Vulnerability R&D Lab today released new vulnerability signatures in the QualysGuard® Web Service to protect enterprises against the new Microsoft® Windows™ DCOM RPC vulnerability. Customers can immediately audit their networks for this new vulnerability by accessing their QualysGuard subscription.

VULNERABILITY DETAIL

The Microsoft RPC DCOM vulnerability (MS03-026, CAN-2003-0352) is a remotely exploitable buffer overflow affecting multiple versions of Microsoft Windows. This vulnerability could potentially allow an attacker to execute malicious code on a vulnerable host. The vulnerability exists in the RPC interface implementing Distributed Component Object Model services (DCOM), which is a vital component of Windows operating systems. By overflowing a buffer in a certain DCOM interface for RPC in Microsoft Windows NT 4.0, 2000, XP, and Server 2003 a remote attacker may gain unauthorized access to vulnerable systems.

For additional information on the Microsoft RPC DCOM Vulnerability, please visit: <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-026.asp>

HOW TO PROTECT YOUR NETWORK

A check for this vulnerability is already available in the QualysGuard Vulnerability assessment platform. A comprehensive scan will detect this issue in addition to over 2,800 other potential vulnerabilities. QualysGuard users can also perform a selective scan for this specific vulnerability using the following check:

- "Microsoft Windows DCOM RPC Interface Buffer Overrun Vulnerability" (Qualys ID: 68518)
 - Limit the scan to TCP ports 135-139 and 445.

TECHNICAL SUPPORT

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

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: <https://qualysguard.qualys.com>