QUALYS
SECURITY ON-DEMAND

ADVISORY

Qualys Security Advisory \ September 10, 2003

Microsoft DCOM RPCSS Service Vulnerability

ADVISORY OVERVIEW

September 10, 2003 - Qualys™ Vulnerability R&D Lab today released a new vulnerability signature in the QualysGuard® Web Service to protect enterprises against the new Microsoft® Windows™ DCOM RPCSS Service vulnerability. Customers can immediately audit their networks for this new vulnerability by accessing their QualysGuard web service.

VULNERABILITY DETAIL

The vulnerability announced in Microsoft Security Bulletin MS03-039 is a remotely exploitable vulnerability similar to the RPC DCOM vulnerability (CAN-2003-0352) recently exploited by the Blaster and Nachi worms. The vulnerability affects all versions of Microsoft Windows and allows a remote attacker to execute malicious code on a compromised host. The RPC patch previously issued by Microsoft as part of Security Bulletin MS03-026 does not address this new vulnerability.

For additional information concerning this vulnerability, please visit the Microsoft Security Bulletin site at:
http://www.microsoft.com/technet/treeview/?url=/technet/security/bulletin/MS03-039.asp

HOW TO PROTECT YOUR NETWORK

A check for this vulnerability is already available in the QualysGuard vulnerability management platform. A comprehensive scan will detect this issue in addition to over 3,000 other potential vulnerabilities. QualysGuard users can also perform a selective scan for this specific vulnerability using the following check:

- "Microsoft Windows DCOM RPCSS Service Vulnerabilities" (Qualys ID: 68522)
  - Limit the scan to TCP ports 135, 139, 445, and 593.
  - If DCOM is enabled over HTTP, include HTTP ports in the scan.

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