QUALYS
SECURITY ON-DEMAND

ADVISORY

Qualys Security Advisory \ August 22, 2003

# Blaster Worm

## ADVISORY OVERVIEW

August 22, 2003 - Qualys™ Vulnerability R&D Lab today advised customers that vulnerability signatures have been available in the QualysGuard® Web Service since July 16, 2003, to protect enterprises against the rapidly spreading MSblast (a.k.a. Blaster) worm. Customers can immediately audit their networks for vulnerability to this worm by accessing their QualysGuard web service.

## WORM DETAIL

Also known as MSBlast, the Blaster worm exploits the Microsoft® RPC DCOM vulnerability (CAN-2003-0352) announced by Microsoft on July 16, 2003, in Microsoft Security Bulletin MS03-0352. 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 remote attacker may gain unauthorized access to vulnerable systems.

For additional information on the Microsoft Windows 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 has been available in the QualysGuard Vulnerability assessment platform since July 16, 2003, the day the vulnerability was announced. A comprehensive scan will detect this issue in addition to almost 3,000 other potential vulnerabilities. QualysGuard users can perform a selective scan for vulnerable and infected hosts using the following checks:

- "Microsoft Windows DCOM RPC Interface Buffer Overrun Vulnerability" (Qualys ID: 68518)

    - While this is an effective technique for detecting vulnerable hosts, detecting infected hosts is more difficult due to instability on port 135 caused by the virus.

- "'msblast.exe' DCOM Worm Detected" (Qualys ID: 90064)
    - Windows login required

Users can also perform a discovery scan against their networks using the TCP services and OS discovery capabilities of QualysGuard, scanning for Windows 2000 and XP hosts that do not respond on TCP port 135.

## 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