QUALYS
SECURITY ON-DEMAND

ADVISORY

Qualys Security Advisory \ January 28, 2003

MS-SQL Slammer Worm

ADVISORY OVERVIEW

January 28, 2003 - Qualys™ Vulnerability R&D Lab today advised customers that vulnerability signatures are available in the QualysGuard® Web Service to protect enterprises against the rapidly spreading MS-SQL Slammer worm. Customers can immediately audit their networks for vulnerability to this worm by accessing their QualysGuard web service.

WORM DETAIL

This self-propagating worm has been spreading rapidly across the Internet since Saturday, January 25, 2003 and has caused severe denial of service attacks against major Internet services ranging from corporate networks to banks' Automatic Teller Machines (ATMs). The worm is exploits buffer overflow vulnerabilities in Microsoft® SQL Server™ announced on July 24, 2002, in Microsoft Security Bulletin MS02-039 (CAN-2002-0649). A host infected with the SQL Slammer worm generates 376-byte UDP packets targeted at UDP port 1434 as it searches for additional vulnerable hosts. This significant increase in UDP traffic results in severe network congestion, in many cases crippling infected networks.

For additional information on the MS-SQL Server Worm, please visit:
http://www.cert.org/advisories/CA-2003-04.html

For information on the Microsoft SQL Server vulnerability exploited by the SQL Slammer worm, please visit:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/alerts/slammer.asp

HOW TO PROTECT YOUR NETWORK

A check for this vulnerability has been available in the QualysGuard Vulnerability assessment platform since July 24, 2002, the day the vulnerability was announced, as part of a the check "Multiple MS-SQL-2000 threats" (Qualys ID: 19062). A

comprehensive scan will detect this issue in addition to over 2,000 other potential vulnerabilities.

A new check has been added to the QualysGuard platform specifically to detect vulnerability to the Slammer worm:

- MS-SQL 8.0 UDP Slammer Worm Buffer Overflow Vulnerability (Qualys ID: 19070)

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