QUALYS
SECURITY ON-DEMAND

ADVISORY

Qualys Security Advisory \ February 10, 2004

Microsoft WINS Vulnerability

ADVISORY OVERVIEW

February 10, 2004 – Qualys™ Vulnerability R&D Lab today announced that it had discovered a denial of service vulnerability in the Microsoft® Windows Internet Naming Service® (WINS). A new signature for this vulnerability was released today in the QualysGuard® Web Service, enabling customers to immediately audit their networks for this and other new vulnerabilities by accessing their QualysGuard subscription.

VULNERABILITY DETAILS

Qualys Vulnerability R&D Lab recently discovered a denial of service vulnerability in Microsoft WINS, described in Microsoft Security Bulletin MS04-006 (CAN-2003-0825). This vulnerability could allow a remote attacker to crash the service or execute malicious code by sending a specially crafted packet to the WINS service on a Windows Server. Microsoft has rated this vulnerability Important and recommends that users patch their WINS servers at the earliest opportunity.

For additional information about affected platforms and available patches, please visit the Microsoft Security Bulletin at:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS04-006.asp

HOW TO PROTECT YOUR NETWORK

A signature for the Microsoft WINS vulnerability discovered by Qualys and announced today by Microsoft is already available in the QualysGuard vulnerability management platform. A default scan will detect this vulnerability. In addition QualysGuard users can perform a selective scan for this specific vulnerability using the following signature:

- "Microsoft WINS Buffer Overflow Vulnerability"
  - Qualys ID: 90104
  - Limit the scan to TCP ports 42, 139 and 445, and UDP port 137
  - 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.

TECHNICAL SUPPORT

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

Additional information about using QualysGuard’s Windows Authentication feature is available in the document “Using Windows Authentication at the Domain Level.” To obtain this document, please visit the Tips & Techniques section of the Resources tab on your QualysGuard Home page.

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