QUALYS
SECURITY ON-DEMAND

ADVISORY

Qualys Security Advisory \ February 10, 2004

Microsoft ASN.1 Vulnerability

ADVISORY OVERVIEW

February 10, 2004 – Qualys™ Vulnerability R&D Lab today released a new vulnerability signature in the QualysGuard® Web Service to protect enterprises against a new Critical-rated Microsoft® Windows™ vulnerability. Customers can immediately audit their networks for this and other new vulnerabilities by accessing their QualysGuard subscription.

VULNERABILITY DETAILS

Microsoft announced the existence of a new Critical-rated buffer overflow vulnerability in the Microsoft Windows ASN.1 library, described in Microsoft Security Bulletin MS04-007. Abstract Syntax Notation 1 (ASN.1) is a data standard that supports the cross-platform normalization and interpretation of data. The ASN.1 library is present in all versions of Windows and is called by a number of important functions, providing a wide variety of potential attack vectors. An attacker exploits this vulnerability by sending malformed data to the ASN.1 library. This vulnerability could give a remote attacker full system privileges on the affected host, allowing them to execute code, view or edit data, and create users.

For additional information about affected platforms and available patches, please visit the Microsoft Security Bulletin at:
http://www.microsoft.com/technet/treeview/?url=/technet/security/bulletin/MS04-007.asp

HOW TO PROTECT YOUR NETWORK

A check for the ASN.1 vulnerability is already available in the QualysGuard vulnerability management platform. A default scan will detect this issue. In addition QualysGuard users can perform a selective scan for this specific vulnerability using the following check:

- "Microsoft ASN.1 Vulnerability"
  - Qualys ID: 90103
  - Limit the scan to TCP ports 139, 443 and 445

- 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