QUALYS
SECURITY ON-DEMAND

ADVISORY

Qualys Security Advisory \ February 2, 2004

Multiple Microsoft Internet Explorer Vulnerabilities

ADVISORY OVERVIEW

February 2, 2004 – Qualys™ Vulnerability R&D Lab today released a new vulnerability signature in the QualysGuard® Web Service to protect enterprises against multiple newly discovered vulnerabilities in Microsoft® Internet Explorer. Customers can immediately audit their networks for these and other new vulnerabilities by accessing their QualysGuard subscription.

VULNERABILITY DETAILS

Microsoft Security Bulletin MS04-004 announces the availability of a cumulative patch for Microsoft Internet Explorer. In addition to superceding the cumulative patch announced in MS03-048, this Critical-rated patch also includes fixes for three previously discovered Internet Explorer vulnerabilities that can allow an attacker to execute malicious code on a vulnerable host.

These new vulnerabilities are:

1. An improper URL canonicalization vulnerability that can allow an attacker to misrepresent the target of a URL in the address bar of an Internet Explorer window. (CAN-2003-1025)

2. A cross-domain vulnerability that could allow an attacker to cause code embedded in an HTML page to execute in the security context of the currently logged-in user. (CAN-2003-1026)

3. A drag-and-drop operation vulnerability that could allow an attacker to save a file to a location on the end-user's computer simply by clicking a hyperlink, without requesting that the end-user approve the download. (CAN-2003-1027)

All of these vulnerabilities could be exploited by an attacker using malicious code embedded in a web page or HTML-formatted email.

For additional information about affected Microsoft platforms and available patches, please visit the Microsoft Security Bulletin at: http://www.microsoft.com/technet/treeview/?url=/technet/security/bulletin/MS04-004.asp

HOW TO PROTECT YOUR NETWORK

A signature for the vulnerabilities announced in Microsoft Security Bulletin MS04-004 is already available in the QualysGuard vulnerability management platform. A default scan will detect these vulnerabilities. In addition QualysGuard users can perform a selective scan for these specific vulnerabilities using the following signature:

- "Microsoft Internet Explorer Cumulative Security Update Not Installed (MS04-004)"
  - Qualys ID: 100004
  - Limit the scan to TCP ports 139 and 445
  - Windows login required
  - Additionally, enable the “Windows Host Name” signature with Qualys ID 82044 if you want to report on infected 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