



Qualys Security Advisory \ November 11, 2003

Multiple Critical Microsoft Vulnerabilities

ADVISORY OVERVIEW

November 11, 2003 – Qualys™ Vulnerability R&D Lab today released new vulnerability signatures in the QualysGuard® Web Service to protect enterprises against the new Microsoft® Windows™ vulnerabilities that were announced earlier today. Customers can immediately audit their networks for these new vulnerabilities by accessing their QualysGuard subscription.

VULNERABILITY DETAIL

Microsoft announced the existence of three new Critical-rated vulnerabilities affecting multiple versions of Microsoft Windows. These vulnerabilities could potentially allow an attacker to execute malicious code on a vulnerable host.

The remotely exploitable vulnerabilities are:

1. MS03-049 (CAN-2003-0812) is a buffer overflow in the Microsoft Windows Workstation service. This service supports communication between Windows clients and network resources such as printers and file servers. All versions of Windows 2000 and Windows XP are vulnerable to this exploit.
2. MS03-051 (CAN-2003-0822) is a buffer overflow in a development interface for Microsoft FrontPage Server Extensions. The vulnerability affects the 2000 and 2002 versions of FrontPage Server Extensions and can allow an attacker to gain full control of a compromised host.

In addition, a critical-rated cumulative update for Microsoft Internet Explorer is now available (MS03-048). This update includes patches for multiple new Internet Explorer vulnerabilities that can be exploited when a user browses a Web site or HTML-formatted email that contains malicious code. These vulnerabilities affect all versions of Microsoft Windows and are a potential avenue of propagation from an email worm.

For additional information concerning these vulnerabilities, please visit Microsoft security bulletin at:

<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/winnov03.asp>

HOW TO PROTECT YOUR NETWORK

Checks for these vulnerabilities are already available in the QualysGuard vulnerability management platform. A comprehensive scan will detect these issues in addition. QualysGuard users can perform a selective scan for these specific vulnerabilities using the following checks:

- "Microsoft Windows Workstation Service Remote Buffer Overflow Vulnerability"
 - Qualys ID: 90078
 - Limit the scan to the following TCP ports 139 and 445
 - Windows login required

- "Microsoft FrontPage Server Extensions Remote Debug Buffer Overrun Vulnerability"
 - Qualys ID: 11329
 - Windows login in not required
 - Limit the scan to any TCP ports using HTTP and HTTPS, including ports 139 and 445

- "Microsoft Internet Explorer Cumulative Security Update Not Installed (MS03-048)"
 - Qualys ID: 100003
 - Windows login required
 - Limit the scan to the following TCP ports 139 and 445

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>