QUALYS
SECURITY ON-DEMAND

ADVISORY

Qualys Security Advisory \ August 22, 2003

W32.Welchia (a.k.a. Nachi) Worm

ADVISORY OVERVIEW

August 22, 2003 - Qualys™ Vulnerability R&D Lab today released new vulnerability signatures in the QualysGuard® Web Service to protect enterprises against the rapidly spreading W32.Welchia worm, also known as the Nachi worm. Customers can immediately audit their networks for this new vulnerability by accessing their QualysGuard web service.

WORM DETAIL

The W32.Welchia (Nachi) worm is a type of "white" worm, a worm that seems benign because it attempts to eradicate the effects and stop the spread of a more visibly malicious worm. The Nachi worm attempts to download the DCOM RPC patch from the Microsoft® web page and install it. It also removes earlier infections from the MSblast worm. The Nachi worm spreads by exploiting either of two vulnerabilities:

1. The Microsoft DCOM RPC vulnerability announced in Microsoft Security Bulletin MS03-026 (CAN-2003-0352). The worm exploits this vulnerability using TCP port 135, and specifically targets Windows XP machines.

2. The WebDAV vulnerability in Microsoft IIS 5.0, announced by Microsoft in Security Bulletin MS03-007 (CAN-2003-0109). WebDAV is an extension of the HTTP protocol (default port 80) that enables users to manage and collaboratively edit files on remote servers. WebDAV fails to perform sufficient bounds checking, allowing a buffer overrun. The worm exploits this vulnerability using TCP port 80.

A computer infected with Nachi generates a large amount of ICMP traffic as the worm probes for other live hosts, resulting in congestion on infected networks due to the significant increase in ICMP traffic.

Please visit the Microsoft web site for additional information about these issues:

- RPC DCOM vulnerability: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-026.asp

- WebDAV vulnerability: http://www.microsoft.com/technet/treeview/?url=/technet/security/bulletin/MS03-007.asp

- Nachi worm: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/alerts/nachi.asp

HOW TO PROTECT YOUR NETWORK

Checks that detect these vulnerabilities and infected hosts are already available in the QualysGuard Vulnerability assessment platform. A comprehensive scan will detect this issue in addition to almost 3,000 other potential vulnerabilities. QualysGuard users can perform selective scans for these specific issues using the following checks:

- "Microsoft Windows DCOM RPC Interface Buffer Overrun Vulnerability" (Qualys ID: 68518)
  - Limit the scan to TCP ports 135-139 and 445

- "Microsoft Windows 2000 IIS WebDAV Buffer Overflow Vulnerability" (Qualys ID: 86479)
  - Limit the scan to port 80 and any other IIS ports running HTTP

- "Nachi Worm Detected" (Qualys ID: 1113)
  - Limit the scan to TCP ports 135-139 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