QUALYS
SECURITY ON-DEMAND

ADVISORY

Qualys Security Advisory \ June 08, 2004

Microsoft Vulnerabilities: DirectPlay and Crystal Reports Web Viewer

ADVISORY OVERVIEW

June 08, 2004 – Qualys™ Vulnerability R&D Lab has released new vulnerability signatures in the QualysGuard® Web Service to protect organizations against new Microsoft® vulnerabilities that were announced earlier today. Customers can immediately audit their networks for these and other new vulnerabilities by accessing their QualysGuard subscription.

VULNERABILITY DETAILS

Microsoft's June 2004 Security Bulletin announced the existence of new vulnerabilities affecting multiple versions of Microsoft Windows and Crystal Reports Web Viewer. These vulnerabilities could potentially allow an attacker to cause a denial of service or retrieve and delete files on vulnerable hosts.

These new vulnerabilities include:

1. A vulnerability in Microsoft® Windows DirectPlay, described in Microsoft Security Bulletin MS04-0016 (CAN-2004-0202). This vulnerability could allow a remote attacker to crash the application by sending a specially crafted packet to the IDirectPlay4 Application Programming Interface (API) of Microsoft DirectPlay. Microsoft has rated this vulnerability Moderate and recommends that users consider applying the security update immediately. http://www.microsoft.com/technet/security/bulletin/MS04-016.mspx

2. A vulnerability in Microsoft® Crystal Reports Web Viewer, described in Microsoft Security Bulletin MS04-0017 (CAN-2004-0204). This vulnerability could allow an attacker who successfully exploited the vulnerability to retrieve and delete files through the Crystal Reports and Crystal Enterprise Web viewers on an affected system. Microsoft has rated this vulnerability Moderate and recommends that users consider applying the security update immediately. http://www.microsoft.com/technet/security/bulletin/MS04-017.mspx

HOW TO PROTECT YOUR NETWORK

Audits for the Microsoft June 2004 Security Bulletin vulnerabilities are already available in the QualysGuard vulnerability management platform. A default scan using authentication will detect these issues and is the recommended detection method. In addition QualysGuard users can perform a selective scan for these specific vulnerabilities using the following checks:

- **"DirectPlay Denial Of Service (MS04-016)"**
  - Qualys ID: 90112
  - 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 vulnerable hosts by Windows (NetBIOS) machine name.

- **"Crystal Reports Web Viewer Information Disclosure/Denial of Service (MS04-017)"**
  - Qualys ID: 90113
  - 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 vulnerable hosts by Windows (NetBIOS) machine name.

TECHNICAL SUPPORT

For more information, customers may contact Qualys Technical Support directly at support@qualys.com or by telephone toll free at:
US: 1 866.801.6161 | EMEA: 33 1 44.17.00.41 | UK: +44 1753 872102

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/trials/qualysguard_trial/