

New Critical Vulnerability in Microsoft Data Access Components (MDAC) Function Which Can Be Exploited via Internet Explorer

Introduction

This vulnerability was discovered by Finjan's Malicious Code Research Center. Vital Security™ Web Appliance is the only product that proactively protects users against this vulnerability.

A remote code execution vulnerability exists in the RDS.Dataspace ActiveX object that is provided as part of the ActiveX Data Objects (ADO) and distributed in MDAC. The RDS is used to move data from a server to a client application or Web page, to manipulate the data on the client, and to return updates to the server in a single round trip.

An attacker who successfully exploits this vulnerability could gain the same user rights as the local user. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrator user rights.

This vulnerability holds for a default installation of a fully patched Windows XP SP2 system with Internet Explorer set to the default security configuration.

Threat level: Critical (Remote Code Execution).

Status: Patched. Microsoft Security Bulletin MS06-014

Affected Products

- Microsoft Windows XP Service Pack 1
- Microsoft Windows XP Service Pack 2
- Microsoft Windows Server 2003
- Microsoft Windows Server 2003 Service Pack 1
- Microsoft Windows Server 2003 for Itanium-based Systems and Microsoft Windows Server 2003 with SP1 for Itanium-based Systems
- Microsoft Windows XP Professional x64 Edition
- Microsoft Windows Server 2003 x64 Edition
- Microsoft Windows 98, Microsoft Windows 98 Second Edition (SE), and Microsoft Windows Millennium Edition (ME)

Attack Vector

- Web and Email attack vectors can be used

Protection

- Vital Security Web Appliance customers are proactively protected against this vulnerability
- Microsoft has provided a patch on 11-April-2006, see [Microsoft Security bulletin MS06-014](#)

Finjan's Solution

Utilizing its patented behavior-based security technologies, Finjan delivers the ONLY proactive content security solution capable of protecting companies from new, unknown attacks arriving via the web the first time they strike. Using this patented technology, Finjan's Vital Security™ solutions provide superior protection against complex web-borne attacks, such as Spyware, Phishing/Pharming, Trojans and malicious code.