

TopResponse Threat Advisory

Release Date: January 11, 2010.

Purpose: The Top Layer TopResponse team is issuing an advisory, which provides information needed to provide protection for the Microsoft Data Access Components ADO Record Memory Vulnerability (MS11-002,CVE-2011-0027).

Top Layer Products: IPS 5500 E-Series.

Vulnerable Infrastructure: Microsoft Data Access Components v2.8 SP1 on Windows XP SP3, Microsoft Data Access Components v2.8 SP2 on Windows XP Professional x64 Edition SP2, Microsoft Data Access Components v2.8 SP2 on Windows Server 2003 SP2, Microsoft Data Access Components v2.8 SP2 on Windows Server 2003 x64 Edition SP2, Microsoft Data Access Components v2.8 SP2 on Windows Server 2003 with SP2 for Itanium-based Systems ,and other software versions as described in the Microsoft bulletin for the vulnerability.

Alert Type: Critical Vulnerability

Risk Assessment: Critical

Threat Impact: Remotely exploitable vulnerability that could allow an attacker to control vulnerable systems

Advisory Impact: Prevention

Summary: Microsoft Data Access Components (MDAC) is a collection of components that make it easy for programs to access databases and then to manipulate the data within them. There exists a vulnerability in the way some of the properties of the ActiveX Data Objects included as part of MDAC are implemented. The reported vulnerability could allow an attacker to execute arbitrary code on the users systems in the context of the logged-on user by enticing the user to visit a specially crafted web site.

Recommended Action: Top Layer recommends the following actions:

Download and apply Protection Pack 2011-01-11-01 (or later) to put this new protection into place. This will put into place protection for the Microsoft Data Access Components ADO Record Memory Vulnerability that will be applied to the "Strict Client Protection" IPS Rule Set.

In order to take advantage of the protection provided in this Protection Pack, make sure the IPS rule tln-106346 is enabled in the IPS Rule Set used to inspect traffic to your Microsoft Access Components infrastructure.

Note: IPS rule tln-106346 is currently enabled in the Strict IPS Rule Set because there is a potential for false positive events. Please monitor events after the rules are enabled to provide protection for this vulnerability.

References: Use the following sources for additional information:

Additional Information	Location
Top Layer Support	http://www.toplayer.com/support
Microsoft Advisory	http://www.microsoft.com/technet/security/bulletin/ms11-002.msp

Relevant TLN Rules: tln-106346.

Relevant TopResponse Protection Pack(s): 2011-01-11-01