

TopResponse Threat Advisory

Release Date: February 9, 2010

Update Date: June 9, 2010

Purpose: The Top Layer TopResponse team is issuing an advisory, which provides information needed to provide updated protection for the Microsoft Data Analyzer ActiveX Control Vulnerability (MS10-034, MS10-008, CVE-2010-0252).

Top Layer Products: IPS 5500 E-Series running V5.18.002 (or later).

Vulnerable Infrastructure: Microsoft Data Analyzer ActiveX Control.

Alert Type: Critical Vulnerability

Risk Assessment: Critical

Threat Impact: Remotely exploitable vulnerability that could allow an attacker to write or delete arbitrary files on the vulnerable systems

Advisory Impact: Prevention

Summary: The Microsoft Data Analyzer ActiveX Control provides application developers a method to programmatically control the Data Analyzer. The vulnerability could allow an attacker to execute arbitrary code on the user's system in the context of the logged-on user by enticing the user to open a specially crafted web page.

Recommended Action: Top Layer recommends the following actions:

Download and apply Protection Pack 2010-06-08-03 (or later) to put this updated protection into place. This is automatically applied to the "Recommended Client Protection" and "Recommended Server Protection" IPS Rule Sets. In order to take advantage of the protection, customers should make sure the IPS rule tln-106297 is enabled in the IPS Rule Set used to inspect traffic that transfers HTML traffic to your infrastructure.

Note: In order to take advantage of the protection provided by these rules, IPS 5500 software version V5.18.002 or higher is required.

References: Use the following sources for additional information:

Additional Information	Location
Top Layer Support	http://www.toplayer.com/support
Microsoft Support	http://www.microsoft.com/technet/security/bulletin/ms10-008.msp http://www.microsoft.com/technet/security/bulletin/ms10-034.msp
Mitre CVE	http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0252

Relevant TLN Rules: tln-106297

Relevant TopResponse Protection Packs: 2010-02-09-01 / 2010-06-08-03

Relevant Top Layer Software Version(s): V5.18.002 or later