



Securing Tomorrow's
Networks Today

TopResponse Threat Advisory

Release Date: August 11, 2010.

Purpose: The Top Layer TopResponse team is issuing an advisory, which provides information needed to provide protection for the Microsoft Word RTF Parsing Engine Memory Corruption (MS10-056,CVE-2010-1901) and Microsoft Word RTF Parsing Buffer Overflow (MS10-056,CVE-2010-1902) Vulnerabilities.

Top Layer Products: IPS 5500 E-Series.

Vulnerable Infrastructure: Microsoft Internet Explorer 6 for Windows XP SP3, Microsoft Internet Explorer 6 for Windows XP Professional x64 Edition SP2, Microsoft Internet Explorer 6 for Windows Server 2003 SP2, Microsoft Internet Explorer 6 for Windows Server 2003 x64 Edition SP2, Microsoft Internet Explorer 6 for Windows Server 2003 with SP2 for Itanium-based Systems, Microsoft Internet Explorer 7, and other software as specified in the Microsoft bulletin describing the vulnerability.

Alert Type: Critical Vulnerabilities

Risk Assessment: Critical

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

Advisory Impact: Prevention

Summary: Microsoft Office Word provides a capability of opening RTF files containing rich text data. While opening RTF files, Microsoft Office Word performs data validation checks on the input rich text data. The data validation checks performed are insufficient and result in vulnerabilities. The reported Microsoft Office Word RTF Parsing vulnerabilities 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 open a specially crafted RTF file.

Recommended Action: Top Layer recommends the following actions:

IPS 5500 E-Series Users:

Download and apply Protection Pack 2010-08-11-02 (or later) to put this new protection into place. This will put into place protection for the Microsoft Word RTF Parsing Engine Memory Corruption and Microsoft Word RTF Parsing Buffer Overflow Vulnerabilities that will be applied to the "Recommended Client Protection" IPS Rule Set.

In order to take advantage of the protection provided in this Protection Pack, make sure the IPS rules tln-106325 and tln-106326 are enabled in the IPS Rule Set used to inspect traffic to your web client infrastructure.

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/MS10-056.msp

Relevant TLN Rules: tln-106325, tln-106326

Relevant TopResponse Protection Pack(s): 2010-08-11-02