



Securing Tomorrow's  
Networks Today

## TopResponse Threat Advisory

**Release Date:** October 14, 2010.

**Purpose:** The Top Layer TopResponse team is issuing an advisory, which provides information needed to provide protection for the Microsoft Internet Explorer DOC Memory Corruption Vulnerability (MS10-071,CVE-2010-3329).

**Top Layer Products:** IPS 5500 E-Series.

**Vulnerable Infrastructure:** Microsoft Internet Explorer v6, Microsoft Internet Explorer v7, Microsoft Internet Explorer v8.

**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 Internet Explorer contains functionality that makes it possible to open Microsoft Word files. 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 web site that contains a specially crafted DOC file.

**Recommended Action:** Top Layer recommends the following actions:

### **IPS 5500 E-Series Users:**

Download and apply Protection Pack 2010-10-11-02 (or later) to put this new protection into place. This will put into place protection for the Microsoft Internet Explorer DOC Memory Corruption Vulnerability 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 rule tln-106332 is 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	<a href="http://www.toplayer.com/support">http://www.toplayer.com/support</a>
Microsoft Advisory	<a href="http://www.microsoft.com/technet/security/bulletin/ms10-071.msp">http://www.microsoft.com/technet/security/bulletin/ms10-071.msp</a>

**Relevant TLN Rules:** tln-106332

**Relevant TopResponse Protection Pack(s):** 2010-10-11-02