

TopResponse Threat Advisory

Release Date: June 16, 2011.

Purpose: The Corero TopResponse team is issuing an advisory, which provides information needed to provide protection for the Microsoft IE Drag and Drop Memory Corruption Vulnerability (MS11-050,CVE-2011-1254).

Corero Products: Top Layer IPS 5500 E-Series and later.

Vulnerable Infrastructure: Microsoft Internet Explorer v6, v7, and 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 a vulnerability in the layout handling implementation. The vulnerability can be triggered by attempts to access uninitialized or deleted objects. The reported vulnerability could allow an attacker to execute arbitrary code on the users systems in the context of the logged-on user.

Recommended Action:

Download and apply Protection Pack 2011-06-15-02 (or later) to put this new protection into place. This will put into place protection for the Microsoft IE Drag and Drop 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-106364 is enabled in the IPS Rule Set used to inspect traffic to your Microsoft IE client infrastructure.

Note: IPS rule tln-106364 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
Corero Support	http://www.corero.com/support
Microsoft Advisory	http://www.microsoft.com/technet/security/Bulletin/MS11-050.msp

Relevant IPS 5500 Rules: tln-106364.

Relevant TopResponse Protection Pack(s): 2011-06-15-02.