

TopResponse Threat Advisory

Release Date: August 15, 2011.

Purpose: The Corero TopResponse team is issuing an advisory, which provides information needed to provide protection for the Microsoft IE Style Object Memory Corruption Vulnerability (MS11-057,CVE-2011-1964).

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

Vulnerable Infrastructure: Microsoft Internet Explorer v6, v7, v8, and v9 as described in the corresponding Microsoft bulletin.

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 supports defining styles for various HTML elements. The defined styles can be dynamically modified by changing behaviors associated with the styles. There exists a vulnerability in the Microsoft IE HTML processing functions pertaining to changing behaviors of certain style elements. 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: Corero recommends the following actions:

Download and apply Protection Pack 2011-08-12-01 (or later) to put this new protection into place. This will put into place protection for the Microsoft IE Style Object Memory Corruption 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-106369 is enabled in the IPS Rule Set used to inspect traffic to your infrastructure vulnerable to the Microsoft IE Style Object Memory Corruption.

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/ms11-057.msp

Relevant IPS 5500 Rules: tln-106369.

Relevant TopResponse Protection Pack(s): 2011-08-12-01.