

## Threat Update Service\* Advisory

### July 10, 2012

**Purpose:** The Corero Security Active Response Team informs customers that existing IPS 5500 security features provide proactive protection against potential attacks targeting the Microsoft Visual Basic for Applications Insecure Library Loading Vulnerability.

**Issue:** Microsoft Visual Basic for Applications does not properly restrict the path used for loading external libraries. This could allow an attacker to execute arbitrary code on the victim's machine. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

**Recommended Action:** Apply the specified protection pack (or any later one) and ensure the associated rule is used to inspect traffic to the affected product infrastructure.

<b>Issue Identifier</b>	CVE-2012-1854, MS12-046
<b>Vendor Advisory</b>	<a href="http://technet.microsoft.com/security/bulletin/MS12-046">http://technet.microsoft.com/security/bulletin/MS12-046</a>
<b>Identified In</b>	July 2012 Microsoft Patch Tuesday release
<b>Risk Assessment</b>	Critical Vulnerability
<b>Threat Impact</b>	Remotely exploitable vulnerability that could allow an attacker to gain full control of an unprotected system.
<b>Affected Products</b>	Microsoft Office 2003 Service Pack 3 Microsoft Office 2007 Service Packs 2 and 3 Microsoft Office 2010 including Service Pack 1 (32-bit and 64-bit editions) Microsoft Visual Basic for Applications Microsoft Visual Basic for Applications SDK
<b>Corero Products</b>	IPS 5500 E-Series and later.
<b>Associated Rule</b>	tln-102004
<b>Associated Rule Set</b>	This rule is automatically enabled in the "Strict Server Protection" rule set.

\* previously called TopResponse

<https://support.corero.com> Corero Network Security, Inc.  
One Cabot Road, Hudson, MA 01749 +1-978-212-1500 • Fax +1-978-212-1600  
• USA • Japan • Asia Pacific • EMEA Copyright 2012. All Rights Reserved.