

Threat Update Service* Advisory

Protection Pack 2012-08-16-02 Released August 16, 2012

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against potential attacks targeting the Microsoft MSCOMCTL.OCX Remote Code Execution Vulnerability.

Issue: An ActiveX control in the Windows common controls corrupts system memory thereby allowing remote code execution. This could allow an attacker to execute arbitrary code on the victim's machine by enticing the victim to open a specially crafted website or a document. 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.

Issue Identifier	CVE-2012-1856, MS12-060
Vendor Advisory	http://technet.microsoft.com/security/bulletin/MS12-060
Identified In	August 2012 Microsoft Patch Tuesday release
Risk Assessment	Critical Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to gain full control of an unprotected system.
Affected Products	<p>Microsoft Office 2003 Service Pack 3 (including Web Components Service Pack 3)</p> <p>Microsoft Office 2007 Service Packs 2 and 3</p> <p>Microsoft Office 2010 Service Pack 1 (32-bit editions)</p> <p>Microsoft SQL Server 2000 Service Pack 4</p> <p>Microsoft SQL Server 2000 Analysis Services Service Pack 4</p> <p>Microsoft SQL Server 2005 Express Edition with Advanced Services Service Pack 4</p> <p>Microsoft SQL Server 2005 for 32-bit, 64-bit and Itanium based Systems Service Pack 4</p> <p>Microsoft SQL Server 2008 for 32-bit, 64-bit and Itanium based Systems Service Packs 2 and 3</p> <p>Microsoft SQL Server 2008 R2 for 32-bit, 64-bit and Itanium based Systems (including Service Pack 1)</p> <p>Microsoft Commerce Server 2002 Service Pack 4</p> <p>Microsoft Commerce Server 2007 Service Pack 2</p> <p>Microsoft Commerce Server 2009 (including R2)</p> <p>Microsoft Host Integration Server 2004 Service Pack 1</p> <p>Microsoft Visual FoxPro 8.0 Service Pack 1</p> <p>Microsoft Visual FoxPro 9.0 Service Pack 2</p> <p>Visual Basic 6.0 Runtime</p>

<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.

Corero Products	IPS 5500 E-Series and later.
Associated Rule	tln-106496
Associated Rule Set	This rule is automatically enabled in the “Strict Client 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.