Threat Update Service* Advisory

Protection Pack 2013-11-06-04 Released November 6, 2013

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the Microsoft Word CVE-2013-3906 Integer Overflow Vulnerability.

Issue: An integer overflow vulnerability exists in Microsoft Windows, Microsoft Office, and Microsoft Lync as they do not properly parse TIFF files. This could allow a remote attacker to execute arbitrary code on the vulnerable machine via a specially crafted file or website.

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-2013-3906
Advisory	http://technet.microsoft.com/en-us/security/advisory/2896666
Risk Assessment	Critical Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to execute arbitrary code on an unprotected system.
Affected Products	Windows Vista Windows Server 2008 Microsoft Office 2003 Microsoft Office 2007 Microsoft Office 2010 Microsoft Lync 2010 Microsoft Lync 2013 Microsoft Lync Basic 2013
Corero Products	IPS 5500 E-Series v5.34 (build 005 and later), v6.60 (build 047 and later), v6.61 (build 021 and later), v6.80 (build 035 and later).
Associated Rule	tln-106733
Associated Rule Set	This rule is automatically enabled in the “Recommended Client Protection” rule set.

* previously called TopResponse

