Threat Update Service* Advisory

Protection Pack 2013-09-18-01 Released September 18, 2013

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against potential attacks targeting the Microsoft Office CVE-2013-3850 Memory Corruption Vulnerability.

Issue: Microsoft Office does not properly parse crafted files thereby corrupting system memory. This could allow an attacker to execute arbitrary code on the victim's machine by enticing the victim to open a specially crafted file. 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-2013-3850, MS13-072
Advisory	http://technet.microsoft.com/en-us/security/bulletin/ms13-072
Risk Assessment	Critical Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to gain full control of an unprotected system.
Affected Products	Microsoft Word 2003 Service Pack 3 Microsoft Word 2007 Service Pack 3 Microsoft Word 2010 Service Pack 1 (32-bit editions) Microsoft Word 2010 Service Pack 1 (64-bit editions) Microsoft Word 2010 Service Pack 2 (32-bit editions) Microsoft Office Compatibility Pack Service Pack 3 Microsoft Word Viewer
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-106699
Associated Rule Set	This rule is automatically enabled in the "Strict Client Protection" rule set.

* previously called TopResponse

