Threat Update Service* Advisory
February 15, 2013

Purpose: The Corero Security Active Response Team informs customers that existing IPS 5500 security features provide proactive protection against potential attacks targeting the Microsoft OLE Automation Remote Code Execution Vulnerability.

Issue: Microsoft Object Linking and Embedding (OLE) Automation does not properly allocate memory when parsing a RTF file. This could allow an attacker to execute arbitrary code on the victim's machine and possibly take complete control of the system.

Recommended Action: Enable the specified rule and ensure that the rule is used to inspect traffic to the affected product infrastructure.

Issue Identifier	CVE-2013-1313, MS13-020
Vendor Advisory	http://technet.microsoft.com/security/bulletin/MS13-020
Risk Assessment	Critical Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to gain full control of an unprotected system.
Affected Products	Windows XP Service Pack 3
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