Threat Update Service* Advisory
March 12, 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 Internet Explorer CTreeNode Use-After-Free Vulnerability.

Issue: Internet Explorer tries to access an object that has been deleted 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 website. An attacker who successfully exploited this vulnerability could take complete control of an affected 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-2013-1288, MS13-021
Vendor Advisory	http://technet.microsoft.com/security/bulletin/MS13-021
Risk Assessment	Critical Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to gain full control of an unprotected system.
Affected Products	Internet Explorer 8
Corero Products	IPS 5500 E-Series and later.
Associated Rule	tln-106585
Associated Rule Set	This rule is automatically enabled in the "Recommended 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