

Threat Update Service* Advisory

Protection Pack 2012-09-28-03 Released September 28, 2012

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against potential attacks targeting the Microsoft Internet Explorer OnMove Use-After-Free Vulnerability.

Issue: Internet Explorer tries to access an object that has not been initialized or 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: 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-2012-1529, MS12-063
Vendor Advisory	http://technet.microsoft.com/security/bulletin/MS12-063
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 6 Internet Explorer 7 Internet Explorer 8 Internet Explorer 9
Corero Products	IPS 5500 E-Series and later.
Associated Rule	tln-106517
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 Copyright 2012. All Rights Reserved.