

Threat Update Service* Advisory
Protection Pack 2015-02-13-01 Released February 13, 2015

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the Microsoft Internet Explorer CVE-2015-0071 Security Bypass Vulnerability.

Issue: A security bypass vulnerability exists in Internet Explorer. This could allow an attacker to bypass ASLR (Address Space Layout Randomization) protection and gain access to sensitive information which could be used in conjunction with another vulnerability to execute arbitrary code on the victim's machine by enticing the victim to open a specially crafted 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-2015-0071, MS15-009
Advisory	https://technet.microsoft.com/en-us/library/security/ms15-009.aspx
Risk Assessment	Critical Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to bypass security protections on an unprotected system.
Affected Products	Internet Explorer 9 Internet Explorer 10 Internet Explorer 11
Corero Products	IPS 5500 EC-Series and IPS 5500 ES-Series v6.82 (build 003 and later).
Associated Rule	tln-107013
Associated Rule Set	This rule is automatically enabled in the "Recommended Client Protection" rule set.

* previously called TopResponse

<http://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 2014. All Rights Reserved.