Threat Update Service* Advisory

Protection Pack 2014-11-12-01 Released November 12, 2014

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against potential attacks targeting the Windows OLE Automation Array Remote Code Execution Vulnerability.

Issue: Internet Explorer tries to improperly access an object in memory 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-2014-6332, MS14-064
Advisory	http://technet.microsoft.com/en-us/security/bulletin/ms14-064
Risk Assessment	Critical Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to execute arbitrary code on an unprotected system.
Affected Products	Windows Server 2003 Windows Vista Windows Server 2008 Windows 7 Windows Server 2008 R2 Windows 8 and Windows 8.1 Windows Server 2012 and Windows Server 2012 R2 Windows RT and Windows RT 8.1
Corero Products	IPS 5500 EC-Series and IPS 5500 ES-Series v6.82 (build 003 and later).
Associated Rule	tln-106963
Associated Rule Set	This rule has to be manually enabled.

* previously called TopResponse

