Threat Update Service* Advisory

Protection Pack 2013-04-09-03 Released April 9, 2013

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against potential attacks targeting the Microsoft Windows RDP ActiveX Control Remote Code Execution Vulnerability.

Issue: The Remote Desktop ActiveX control mstscax.dll 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: 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-2013-1296, MS13-029
Advisory	http://technet.microsoft.com/security/bulletin/MS13-029
Risk Assessment	Critical Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to gain full control of an unprotected system.
Affected Products	Remote Desktop Connection 6.1 Client Remote Desktop Connection 7.0 Client
Corero Products	IPS 5500 E-Series and later.
Associated Rule	tln-106607
Associated Rule Set	This rule is automatically enabled in the "Recommended Client Protection" rule set.

* previously called TopResponse

