

Threat Update Service* Advisory

Protection Pack 2013-12-09-02 Released December 10, 2013

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

Issue: The Microsoft Scripting Runtime Object Library 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-2013-5056, MS13-099
Advisory	http://technet.microsoft.com/en-us/security/bulletin/ms13-099
Risk Assessment	Critical Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to gain full control of an unprotected system.
Affected Products	Windows XP Windows Server 2003 Windows Vista Windows Server 2008 Windows 7 Windows 8 and Windows 8.1 Windows 2012 and Windows Server 2012 R2 Windows RT and Windows RT 8.1
Corero Products	IPS 5500 E-Series v5.34 (build 005 and later), v6.60 (build 047 and later), v6.61 (build 021 and later), v6.80 (build 035 and later).
Associated Rule	tln-106762
Associated Rule Set	This rule is automatically enabled in the "Strict Client Protection" rule set.

* previously called TopResponse