Threat Update Service* Advisory

Protection Pack 2013-09-27-05 Released September 27, 2013

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the Microsoft Windows CVE-2013-0810 Theme File Handling Vulnerability.

Issue: A remote code execution vulnerability exists in Microsoft Windows. This could allow an attacker to execute arbitrary code on the system and possibly take complete control of the system via a specially crafted screensaver in a theme file.

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-2013-0810, MS13-071
Advisory	http://technet.microsoft.com/en-us/security/bulletin/ms13-071
Risk Assessment	Critical Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to execute arbitrary code on the system.
Affected Products	Microsoft Windows XP SP2 and SP3 Windows Server 2003 SP2 Windows Vista SP2 Windows Server 2008 SP2
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-022180
Associated Rule Set	This rule is automatically enabled in the “Recommended Client Protection” rule set.

* previously called TopResponse

