Threat Update Service* Advisory

Protection Pack 2014-10-20-02 Released October 20, 2014

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

Issue: Microsoft .NET Framework does not properly parse internationalized resource identifiers. This could allow an attacker to execute arbitrary code on the victim's machine by enticing the victim to open a specially crafted file. 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-2014-4121, MS14-057
Advisory	http://technet.microsoft.com/en-us/security/bulletin/ms14-057
Risk Assessment	Critical Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to execute arbitrary code on an unprotected system.
Affected Products	Microsoft .NET Framework 2.0 Service Pack 2 Microsoft .NET Framework 3.5 Microsoft .NET Framework 3.5.1 Microsoft .NET Framework 4 Microsoft .NET Framework 4.5/4.5.1/4.5.2
Corero Products	IPS 5500 EC-Series and IPS 5500 ES-Series v6.60 (build 047 and later), v6.61 (build 021 and later), v6.80 (build 035 and later), v6.82 (build 003 and later).
Associated Rule	tln-106950
Associated Rule Set	This rule is automatically enabled in the "Recommended Client Protection" rule set.

* previously called TopResponse

