Threat Update Service* Advisory

Protection Pack 2013-05-28-01 Released May 28, 2013

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against potential attacks targeting the Microsoft .NET Framework XML Digital Signature Spoofing Vulnerability.

Issue: The Microsoft .NET Framework CLR does not properly validate the signature of XML files. This could allow an attacker to modify the contents of the XML file without invalidating the signature thereby carrying out a spoofing attack.

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-2013-1336, MS13-040
Advisory	http://technet.microsoft.com/en-us/security/bulletin/ms13-040
Risk Assessment	Important Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to spoof the contents of an XML file without invalidating its signature.
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
Corero Products	IPS 5500 E-Series and later.
Associated Rule	tln-106626
Associated Rule Set	This rule is automatically enabled in the “Recommended Client Protection” rule set.

* previously called TopResponse

https://support.corero.com Corero Network Security, Inc.
One Cabot Road, Hudson, MA 01749 +1 978.212.1500 • Fax +1 978.212.1600
• USA • Japan • Asia Pacific • EMEA