

Threat Update Service* Advisory

Protection Pack 2014-07-17-02 Released July 18, 2014

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the Microsoft .NET Framework CVE-2014-0257 Remote Privilege Escalation Vulnerability.

Issue: Microsoft .NET Framework does not properly determine whether it is safe to execute a method or not. This could allow an attacker to execute arbitrary code on the victim's machine by enticing the victim to open a specially crafted website or a crafted .NET Framework application that exposes a COM server endpoint. 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-2014-0257, MS14-009
Advisory	http://technet.microsoft.com/en-us/security/bulletin/ms14-009
Risk Assessment	Important Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to execute arbitrary code on an unprotected system.
Affected Products	Microsoft .NET Framework 1.0 SP3, 1.1 SP1, 2.0 SP2, 3.5, 3.5.1, 4, 4.5, and 4.5.1
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	tIn-025267
Associated Rule Set	This rule is automatically enabled in the "Recommended Client Protection" rule set.

* previously called TopResponse

<http://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 Copyright 2014. All Rights Reserved.