Threat Update Service* Advisory

Protection Pack 2013-01-11-01 Released January 11, 2013

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against potential attacks targeting the Microsoft .NET System.DirectoryServices.Protocols Buffer Overflow Vulnerability.

Issue: The System.DirectoryServices.Protocols (S.DS.P) namespace method in the .NET Framework does not properly validate the size of objects before copying them into an array. This could allow an attacker to execute arbitrary code on the victim's machine. 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-2013-0003, MS13-004
Vendor Advisory	http://technet.microsoft.com/security/bulletin/MS13-004
Risk Assessment	Critical Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to gain full control of an unprotected system.
Affected Products	Microsoft .NET Framework 2.0 Service Pack 2 Microsoft .NET Framework 3.0 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-509011
Associated Rule Set	This rule needs to be specifically applied for it to be enabled.

* 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 Copyright 2012. All Rights Reserved.