Threat Update Service* Advisory

Protection Pack 2012-08-15-03 Released August 15, 2012

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against potential attacks targeting the Microsoft Windows Remote Desktop Protocol Vulnerability.

Issue: The Remote Desktop Protocol implementation on Windows tries to access an object that has been deleted thereby corrupting system memory. 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-2012-2526, MS12-053
Vendor Advisory	http://technet.microsoft.com/security/bulletin/MS12-053
Identified In	August 2012 Microsoft Patch Tuesday release
Risk Assessment	Critical Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to gain full control of an unprotected system.
Affected Products	Windows XP Service Pack 3
Corero Products	IPS 5500 E-Series and later.
Associated Rule	tln-106495
Associated Rule Set	This rule is automatically enabled in the "Recommended Client Protection" and the "Recommended Server Protection" rule sets.

* 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