Threat Update Service* Advisory

Protection Pack 2012-08-24-01 Released August 24, 2012

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against potential attacks targeting the Microsoft Visio DXF File Format Buffer Overflow Vulnerability.

Issue: Microsoft Visio does not properly handle memory when parsing Visio files. This could allow an attacker to execute arbitrary code on the victim's machine by enticing the victim to open a specially crafted Visio 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-2012-1888, MS12-059
Vendor Advisory	http://technet.microsoft.com/security/bulletin/MS12-059
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	Microsoft Visio 2010 Service Pack 1 (32-bit and 64-bit editions) Microsoft Visio Viewer 2010 Service Pack 1 (32-bit and 64-bit editions)
Corero Products	IPS 5500 E-Series and later.
Associated Rule	tln-106491
Associated Rule Set	This rule is automatically enabled in the "Recommended Client Protection" rule set.

* previously called TopResponse

