Threat Update Service* Advisory

Protection Pack 2013-10-21-01 Released October 21, 2013

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the Microsoft DirectShow CVE-2013-3174 Arbitrary Memory Overwrite Vulnerability.

Issue: Microsoft DirectShow does not properly parse GIF files. This could allow an attacker to execute arbitrary code on an affected system by enticing the victim to open a specially crafted GIF 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-2013-3174
Advisory	http://technet.microsoft.com/security/bulletin/MS13-056
Risk Assessment	Critical Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to execute arbitrary code on an unprotected system.
Affected Products	Microsoft Windows XP SP2 and SP3 Windows Server 2003 SP2 Windows Vista SP2 Windows Server 2008 SP2 and R2 SP1 Windows 7 SP1 Windows 8 Windows Server 2012
Corero Products	IPS 5500 E-Series v5.34 (build 005 and later), v6.60 (build 047 and later), v6.61 (build 021 and later), v6.80 (build 035 and later).
Associated Rule	tln-021502
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