Threat Update Service* Advisory
Protection Pack 2012-07-27-01 Released July 27, 2012

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against potential attacks targeting the Apple QuickTime TeXML Style Element Stack Buffer Overflow Vulnerability.

Issue: Apple QuickTime does not properly validate TeXML files. This could allow an attacker to execute arbitrary code on the remote machine by sending a specially crafted TeXML file and enticing the victim to open the 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-2012-0663
Vendor Advisory	http://support.apple.com/kb/HT5261
Risk Assessment	Important Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to gain full control of an unprotected system.
Affected Products	Apple QuickTime before 7.7.2 on Windows
Corero Products	IPS 5500 E-Series and later.
Associated Rule	tln-106487
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