

## **Threat Update Service\* Advisory** **Protection Pack 2012-07-20-02 Released July 24, 2012**

**Purpose:** The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against potential attacks targeting the Apple QuickTime QTVR Files Remote Code Execution Vulnerability.

**Issue:** Apple QuickTime does not properly validate QTVR movie files. This could allow an attacker to execute arbitrary code on the remote machine by sending a specially crafted QTVR 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.

<b>Issue Identifier</b>	CVE-2012-0667
<b>Vendor Advisory</b>	<a href="http://support.apple.com/kb/HT5261">http://support.apple.com/kb/HT5261</a>
<b>Risk Assessment</b>	Important Vulnerability
<b>Threat Impact</b>	Remotely exploitable vulnerability that could allow an attacker to gain full control of an unprotected system.
<b>Affected Products</b>	Apple QuickTime before 7.7.2 on Windows
<b>Corero Products</b>	IPS 5500 E-Series and later.
<b>Associated Rule</b>	tln-022147
<b>Associated Rule Set</b>	This rule is automatically enabled in the "Recommended Client Protection" rule set.

\* previously called TopResponse