

**Threat Update Service\* Advisory**  
**Protection Pack 2013-04-19-03 Released April 19, 2013**

**Purpose:** The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the RealNetworks RealPlayer RealMedia File Handling Buffer Overflow Vulnerability.

**Issue:** A buffer overflow vulnerability exists in RealNetworks RealPlayer. This could allow a remote attacker to execute arbitrary code on the system and possibly take complete control of the affected system via a crafted RealMedia file.

**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-2012-5691
<b>Advisory</b>	<a href="http://service.real.com/realplayer/security/12142012_player/en/">http://service.real.com/realplayer/security/12142012_player/en/</a>
<b>Risk Assessment</b>	Critical Vulnerability
<b>Threat Impact</b>	Remotely exploitable vulnerability that could allow an attacker to execute arbitrary code on the system.
<b>Affected Products</b>	RealNetworks RealPlayer before 16.0.0.282 RealPlayer SP 1.0 through 1.1.5
<b>Corero Products</b>	IPS 5500 E-Series and later.
<b>Associated Rule</b>	tln-106611
<b>Associated Rule Set</b>	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 Copyright 2013. All Rights Reserved.