Threat Update Service* Advisory

Protection Pack 2014-01-08-02 Released January 9, 2014

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the RealPlayer CVE-2013-6877 Heap Based Buffer Overflow Vulnerability.

Issue: A heap buffer overflow vulnerability exists in the RealNetworks RealPlayer. This could allow an attacker to execute arbitrary code on the victim's machine via a long string in the TRACKID element of an RMP 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.

Issue Identifier	CVE-2013-6877
Advisory	http://service.real.com/realplayer/security/12202013_player/en/
Risk Assessment	Critical Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to execute arbitrary code on an unprotected system.
Affected Products	RealNetworks RealPlayer before 17.0.4.61 on Windows RealNetworks RealPlayer before 12.0.1.1738 on Mac
Corero Products	IPS 5500 E-Series v6.60 (build 047 and later), v6.61 (build 021 and later), v6.80 (build 035 and later).
Associated Rule	tln-106771
Associated Rule Set	This rule is automatically enabled in the "Recommended Client Protection" rule set.

* previously called TopResponse

