Threat Update Service* Advisory

Protection Pack 2012-08-09-01 Released August 10, 2012

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the Real Networks RealPlayer QCP Parsing Remote Code Execution Vulnerability.

Issue: A heap buffer overflow exists in qcpfformat.dll in RealNetworks RealPlayer. This could allow an attacker to execute arbitrary code on the remote machine by sending a specially crafted QCP 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-2011-2950
Vendor Advisory	http://service.real.com/realplayer/security/08162011_player/en/
Risk Assessment	Critical Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to gain full control of an unprotected system.
Affected Products	RealNetworks RealPlayer 11.0 through 11.1 RealNetworks RealPlayer 14.0.0 through 14.0.5 RealPlayer SP 1.0 through 1.1.5
Corero Products	IPS 5500 E-Series and later.
Associated Rule	tln-106489
Associated Rule Set	This rule is automatically enabled in the “Recommended Client Protection” rule set.

* previously called TopResponse

