Threat Update Service* Advisory

Protection Pack 2012-11-23-01 Released November 23, 2012

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the NTRglobal NTR ActiveX Control StopModule Remote Code Execution Vulnerability.

Issue: The StopModule method in the NTR ActiveX control does not properly validate input to the lModule parameter thereby allowing the attacker to take control of certain function pointers. This could allow an attacker to execute arbitrary code on the victim's machine by enticing the victim to open a specially crafted website. 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-2012-0267
Advisory	http://secunia.com/advisories/45166
Risk Assessment	Critical Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to gain full control of an unprotected system.
Affected Products	NTR ActiveX control before 2.0.4.8
Corero Products	IPS 5500 E-Series and later.
Associated Rule	tln-106544
Associated Rule Set	This rule is automatically enabled in the "Recommended Client Protection" rule set.

* previously called TopResponse

