Threat Update Service* Advisory

Protection Pack 2013-03-29-03 Released March 29, 2013

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

Issue: A stack buffer overflow vulnerability exists in the NTR ActiveX control as it does not properly validate the bstrParams parameter to the Check method. This could allow a remote attacker to execute arbitrary code on the system and possibly take complete control of the affected system by enticing the victim to open a specially crafted webpage.

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-2012-0266
Advisory	http://secunia.com/advisories/45166
Risk Assessment	Critical Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to execute arbitrary code on the system.
Affected Products	NTR ActiveX control before 2.0.4.8
Corero Products	IPS 5500 E-Series and later.
Associated Rule	tln-025164
Associated Rule Set	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