

Threat Update Service* Advisory
Protection Pack 2013-12-09-02 Released December 10, 2013

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

Issue: A remote code execution vulnerability exists in the StopModule method in the NTR ActiveX control as it does not properly sanitize the IModule parameter. 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://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0267
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 v5.34 (build 005 and later), v6.60 (build 047 and later), v6.61 (build 021 and later), v6.80 (build 035 and later).
Associated Rule	tln-021510
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 Copyright 2013. All Rights Reserved.