Threat Update Service* Advisory

Protection Pack 2013-02-12-03 Released February 12, 2013

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the Novell ZENworks AdminStudio LaunchHelp.dll ActiveX Code Execution Vulnerability.

Issue: A directory traversal vulnerability exists in the LaunchProcess function in the LaunchHelp.HelpLauncher.1 ActiveX control in LaunchHelp.dll in AdminStudio in Novell ZENworks Configuration Management. This could allow an attacker to execute arbitrary code on the victim's machine via a pathname in the first argument. 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-2011-2657
Vendor Advisory	http://www.novell.com/support/kb/doc.php?id=7009570
Risk Assessment	Important Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to gain full control of an unprotected system.
Affected Products	Novell ZENworks Configuration Management 10.2, 10.3, and 11 SP1
Corero Products	IPS 5500 E-Series and later.
Associated Rule	tln-106581
Associated Rule Set	This rule is automatically enabled in the "Recommended Client Protection" rule set.

* previously called TopResponse

