Threat Update Service* Advisory

Protection Pack 2013-02-22-02 Released February 22, 2013

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the Novell GroupWise Client gwcls1.dll ActiveX Remote Code Execution Vulnerability.

Issue: A remote code execution vulnerability exists in the Novell Groupwise Client as it does not properly validate user supplied data. 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-2012-0439
Advisory	http://www.securityfocus.com/bid/57658/discuss
Risk Assessment	Important Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to gain full control of an unprotected system.
Affected Products	Versions prior to Novell GroupWise 8.0.3 Hot Patch 2 Versions prior to Novell GroupWise 2012 SP1 Hot Patch 1
Corero Products	IPS 5500 E-Series and later.
Associated Rule	tln-025158
Associated Rule Set	This rule is automatically enabled in the "Recommended Client Protection" rule set.

* previously called TopResponse

