Threat Update Service* Advisory

Protection Pack 2013-04-26-02 Released April 26, 2013

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the Novell GroupWise Untrusted Pointer Dereference Vulnerability.

Issue: A pointer dereference vulnerability exists in the client in Novell GroupWise. This could allow an attacker to cause a denial of service or 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 possibly 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-2013-0804
Advisory	http://www.novell.com/support/kb/doc.php?id=7011687
Risk Assessment	Critical Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to cause a denial of service or execute arbitrary code on the unprotected system.
Affected Products	Novell GroupWise 8.0 before 8.0.3 HP2 and 2012 before SP1 HP1
Corero Products	IPS 5500 E-Series and later.
Associated Rule	tln-106614
Associated Rule Set	This rule is automatically enabled in the "Recommended Client Protection" rule set.

* previously called TopResponse

