

Threat Update Service* Advisory

Protection Pack 2013-03-01-03 Released March 1, 2013

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the Novell GroupWise HTTP Interfaces Arbitrary File Retrieval Vulnerability.

Issue: A directory traversal vulnerability exists in Novell GroupWise. This could allow an attacker to gain access to sensitive information via a specially crafted HTTP request. An attacker who successfully exploited this vulnerability could read arbitrary files on 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-2012-0419
Vendor Advisory	http://www.novell.com/support/kb/doc.php?id=7010772
Risk Assessment	Important Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to gain access to sensitive information.
Affected Products	Novell GroupWise 8.0 before Support Pack 3 Novell GroupWise 2012 before Support Pack 1
Corero Products	IPS 5500 E-Series and later.
Associated Rule	tln-025159
Associated Rule Set	This rule is automatically enabled in the "Recommended Server Protection" rule set.

* previously called TopResponse