Threat Update Service* Advisory

Protection Pack 2012-10-26-04 Released October 26, 2012

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the Novell ZENworks Configuration Management Preboot Remote File Access Vulnerability.

Issue: A directory traversal vulnerability exists in the Preboot Service in Novell ZENworks Configuration Management. This could allow an attacker to gain access to sensitive files on the remote machine by sending a specially crafted opcode 0x21 request.

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-2012-2215
Vendor Advisory	http://support.novell.com/docs/Readmes/InfoDocument/patchbuilder/readme_5127930.html
Risk Assessment	Important Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to gain access to sensitive information on an unprotected system.
Affected Products	Novell ZENworks Configuration Management 11.1 and 11.1a
Corero Products	IPS 5500 E-Series and later.
Associated Rule	tln-025142
Associated Rule Set	This rule is automatically enabled in the “Recommended Server Protection” rule set.

* previously called TopResponse

