

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 0x6C Buffer Overflow Vulnerability.

Issue: A stack buffer overflow vulnerability exists in the Preboot Service in Novell ZENworks Configuration Management. This could allow an attacker to execute arbitrary code on the victim's machine via a specially crafted opcode 0x6c request. 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-2011-3175
Vendor Advisory	http://www.novell.com/support/viewContent.do?externalId=7010044
Risk Assessment	Critical 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 11.1 and 11.1a
Corero Products	IPS 5500 E-Series and later.
Associated Rule	tIn-021146
Associated Rule Set	This rule is automatically enabled in the "Recommended Server Protection" rule set.

* previously called TopResponse

<https://support.corero.com> Corero Network Security, Inc.
One Cabot Road, Hudson, MA 01749 +1-978-212-1500 • Fax +1-978-212-1600
• USA • Japan • Asia Pacific • EMEA Copyright 2012. All Rights Reserved.