Threat Update Service* Advisory

Protection Pack 2013-01-25-01 Released January 25, 2013

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the Novell NCP Pre-Auth Remote Stack-Based Buffer Overflow Vulnerability.

Issue: A stack buffer overflow vulnerability exists in the Novell NCP implementation in NetIQ eDirectory. This could allow an attacker to execute arbitrary code on the victim's machine. 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-2012-0432
Advisory	http://www.novell.com/support/kb/doc.php?id=3426981
Risk Assessment	Critical Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to gain full control of an unprotected system.
Affected Products	NetIQ eDirectory 8.8.7.x before 8.8.7.2
Corero Products	IPS 5500 E-Series and later.
Associated Rule	tln-106577
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