

Threat Update Service* Advisory

Protection Pack 2012-11-20-02 Released November 20, 2012

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the EMC NetWorker nsrd RPC Service Format String Vulnerability.

Issue: A format string vulnerability exists in the nsrd RPC service in EMC NetWorker. This could allow an attacker to execute arbitrary code on the victim's machine via format string specifiers in a message. 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-2012-2288
Advisory	http://www.securityfocus.com/bid/55330
Risk Assessment	Critical Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to gain full control of an unprotected system.
Affected Products	EMC NetWorker 7.6.3 and 7.6.4 before 7.6.4.1 EMC NetWorker 8.0 before 8.0.0.1
Corero Products	IPS 5500 E-Series and later.
Associated Rule	tln-022159
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.