

Threat Update Service* Advisory
Protection Pack 2013-11-01-03 Released November 4, 2013

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the EMC Replication Manager Command Execution Vulnerability.

Issue: A remote command execution vulnerability exists in the EMC Replication Manager Client. This could allow a remote attacker to execute arbitrary commands on the vulnerable machine via the RunProgram function on TCP port 6542.

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-2011-0647
Advisory	http://www.securityfocus.com/bid/46235
Risk Assessment	Important Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to execute arbitrary commands on an unprotected system.
Affected Products	EMC Replication Manager Client before 5.3 Microsoft Applications 2.1.x and 2.2.x
Corero Products	IPS 5500 E-Series v5.34 (build 005 and later), v6.60 (build 047 and later), v6.61 (build 021 and later), v6.80 (build 035 and later).
Associated Rule	tIn-025205
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 2013. All Rights Reserved.