Threat Update Service* Advisory

Protection Pack 2013-12-03-01 Released December 4, 2013

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the Computer Associates ARCserve D2D Session Handling Vulnerability.

Issue: A remote command execution vulnerability exists in the CA ARCserver D2D as it does not properly handle sessions. This could allow an attacker to execute arbitrary code on the 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-2011-3011
Advisory	https://support.ca.com/irj/portal/anonymous/phpsupcontent?contentID=%7B7D3ACC0F-6C01-4BE2-B5C0-C430CEB45BE6%7D
Risk Assessment	Critical Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to execute arbitrary code on an unprotected system.
Affected Products	CA ARCserve D2D r15
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	tln-021506
Associated Rule Set	This rule is automatically enabled in the “Recommended Server Protection” rule set.

* previously called TopResponse

