Threat Update Service* Advisory

Protection Pack 2014-04-24-06 Released April 25, 2014

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the LANDesk Lenovo ThinkManagement Console Remote Command Execution Vulnerability.

Issue: A file upload vulnerability exists in the ServerSetup web service in Lenovo ThinkManagement Console. This could allow an attacker to execute arbitrary code on the victim's machine by uploading a file with an executable extension via a PutUpdateFileCore command in a RunAMTCommand SOAP request and then requesting it directly.

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-2012-1195
Advisory	http://osvdb.org/79276
Risk Assessment	Critical Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to execute arbitrary code on an unprotected system.
Affected Products	Lenovo ThinkManagement Console 9.0.3
Corero Products	IPS 5500 E-Series v6.60 (build 047 and later), v6.61 (build 021 and later), v6.62 (build 007 and later), v6.80 (build 035 and later).
Associated Rule	tln-025255
Associated Rule Set	This rule is automatically enabled in the "Recommended Server Protection" rule set.

* previously called TopResponse

