Threat Update Service* Advisory

Protection Pack 2015-02-25-01 Released February 25, 2015

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the Lexmark MarkVision Enterprise Arbitrary File Upload Vulnerability.

Issue: A file upload vulnerability exists in Lexmark MarkVision Enterprise. This could allow an attacker to upload and execute arbitrary files on the victim's machine via a specially crafted request.

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-2014-8741
Advisory	http://support.lexmark.com/index?page=content&id=TE666&locale=en&userlocale=EN_US
Risk Assessment	Critical Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to upload arbitrary files to an unprotected system
Affected Products	Lexmark MarkVision Enterprise 2.0 or earlier
Corero Products	IPS 5500 EC-Series and IPS 5500 ES-Series v6.60 (build 047 and later), v6.61 (build 021 and later), v6.80 (build 035 and later), v6.82 (build 003 and later).
Associated Rule	tln-025326
Associated Rule Set	This rule is automatically enabled in the "Recommended Server Protection" rule set.

* previously called TopResponse

