Threat Update Service* Advisory

Protection Pack 2013-08-20-04 Released August 20, 2013

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the Apache CXF CVE-2013-2160 Remote Denial of Service Vulnerability.

Issue: The Apache streaming XML parser does not properly validate user input thereby allowing an attacker to cause a denial of service by sending specially crafted HTTP requests.

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-2013-2160
Advisory	http://cxf.apache.org/security-advisories.data/CVE-2013-2160.txt.asc?version=1&modificationDate=1372324301037
Risk Assessment	Important Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to cause a denial of service of an unprotected system.
Affected Products	Apache CXF prior to 2.5.10, 2.6.7 and 2.7.4
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-106665
Associated Rule Set	This rule is automatically enabled in the “Recommended Server Protection” rule set.

* previously called TopResponse

