Threat Update Service* Advisory

August 6, 2013

Purpose: The Corero Security Active Response Team informs customers that the IPS 5500 has proactive coverage against known attacks targeting the Cisco Linksys E1200 N300 Router 'submit_button' Parameter Cross Site Scripting Vulnerability.

Issue: Cisco Linksys contains a cross-site scripting (XSS) vulnerability that could allow an attacker to inject an arbitrary web script or HTML script that can be executed on the victim's machine. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

Recommended Action: Enable the specified rule and ensure that the rule is used to inspect traffic to the affected product infrastructure.

Issue Identifier	CVE-2013-2679
Advisory	http://www.securityfocus.com/bid/59558/references
Risk Assessment	Important Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to gain full control of an unprotected system.
Affected Products	Cisco Linksys E1200 N300 running firmware 2.0.04
Corero Products	IPS 5500 E-Series v5.34 (build 005 and later), v6.60 (build 047 and later), v6.61 (build 013 and later), v6.80 (build 035 and later).
Associated Rule	tln-102078
Associated Rule Set	This rule is automatically enabled in the "Strict Client Protection" and "Recommended Server Protection" rule sets.

* previously called TopResponse

