# Threat Update Service* Advisory

## Protection Pack 2012-08-02-01 Released August 3, 2012

**Purpose:** The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the Cisco Linksys PlayerPT ActiveX Control Buffer Overflow Vulnerability.

**Issue:** A stack buffer overflow exists in the setSource method of the Cisco Linksys PlayerPT ActiveX control. This could allow an attacker to execute arbitrary code on the remote machine by sending a very long sURL argument to the setSource method. An attacker who successfully exploited this vulnerability could take complete control of an 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-2012-0284 |
| **NVD Advisory** | http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0284 |
| **Risk Assessment** | Critical Vulnerability |
| **Threat Impact** | Remotely exploitable vulnerability that could allow an attacker to gain full control of an unprotected system. |
| **Affected Products** | Cisco Linksys PlayerPT ActiveX Control 1.0.0.15 |
| **Corero Products** | IPS 5500 E-Series and later. |
| **Associated Rule** | tln-022149 |
| **Associated Rule Set** | This rule is automatically enabled in the “Recommended Client Protection” rule set. |

* previously called TopResponse

https://support.corero.com Corero Network Security, Inc.
One Cabot Road, Hudson, MA 01749 +1-978-212-1500 • Fax +1-978-212-1600
• USA • Japan • Asia Pacific • EMEA 