# Threat Update Service* Advisory

## October 6, 2013

**Purpose:** The Corero Security Active Response Team informs customers that the IPS 5500 has proactive coverage against known attacks targeting the FreeFTPD PASS Command Buffer Overflow Vulnerability.

**Issue:** A buffer overflow vulnerability exists in freeFTPd as it does not properly sanitize user supplied input. This could allow an attacker to execute arbitrary code on the system and possibly gain complete control of the system.

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

| | |
|---|---|
| **Issue Identifier** | BID: 61905 |
| **Advisory** | http://www.securityfocus.com/bid/61905 |
| **Risk Assessment** | Important Vulnerability |
| **Threat Impact** | Remotely exploitable vulnerability that could allow an attacker to execute arbitrary code on the system. |
| **Affected Products** | freeFTPd 1.0.10 |
| **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-004005 |
| **Associated Rule Set** | This rule is automatically enabled in the “Recommended Server Protection” and “Recommended Client Protection” rule sets. |

* previously called TopResponse

 