

Threat Update Service* Advisory **Protection Pack 2013-01-25-01 Released January 25, 2013**

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the Astium VoIP PBX Denial-of-Service Vulnerability.

Issue: A buffer overflow vulnerability exists in the astiumd service in Astium VoIP PBX. This could allow an attacker to cause a denial of service of the victim's machine via a specially crafted packet .

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 | BID: 57095 |
| Advisory | http://www.securityfocus.com/bid/57095/ |
| 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 | Astium VoIP PBX v2.1 and earlier versions |
| Corero Products | IPS 5500 E-Series and later. |
| Associated Rule | tln-106576 |
| Associated Rule Set | This rule is automatically enabled in the "Recommended Server 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 Copyright 2012. All Rights Reserved.