Threat Update Service* Advisory

Protection Pack 2014-07-03-01 Released July 3, 2014

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the AT&T Connect Participant Application SVT File Vulnerability.

Issue: A stack buffer overflow vulnerability exists in the AT&T Connect Participant Application. This could allow an attacker to execute arbitrary code on the victim's machine via a specially crafted SVT file. 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-2013-6029
Advisory	http://www.kb.cert.org/vuls/id/346278
Risk Assessment	Critical Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to execute arbitrary code on an unprotected system.
Affected Products	AT&T Connect Participant Application before 9.5.51
Corero Products	IPS 5500 EC-Series and IPS 5500 ES-Series v6.60 (build 047 and later), v6.61 (build 021 and later), v6.80 (build 035 and later), v6.82 (build 003 and later).
Associated Rule	ttln-022198
Associated Rule Set	This rule is automatically enabled in the "Strict Client Protection" rule set.

* previously called TopResponse

