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 ScadaTEC ModbusTagServer and ScadaPhone Remote Buffer Overflow Vulnerability.

Issue: A buffer overflow exists in TurboPower Abbrevia. This could allow an attacker to execute arbitrary code on the remote machine by sending a specially crafted ZIP 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-2011-4535
Advisory	http://www.us-cert.gov/control_systems/pdf/ICSA-11-362-01.pdf
Risk Assessment	Critical Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to gain full control of an unprotected system.
Affected Products	ScadaTEC ScadaPhone 5.3.11.1230 and earlier ScadaTEC ModbusTagServer 4.1.1.81 and earlier TurboPower Abbrevia before 4.0
Corero Products	IPS 5500 E-Series and later.
Associated Rule	tln-022150
Associated Rule Set	This rule is automatically enabled in the “Recommended Client Protection” rule set.

* previously called TopResponse

