



Threat Update Service* Advisory Protection Pack 2013-03-29-03 Released March 29, 2013

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the Schneider Electric Accutech Manager Heap-based Buffer Overflow Vulnerability.

Issue: A heap buffer overflow vulnerability exists in Schneider Electric Accutech Manager. This could allow a remote attacker to execute arbitrary code on the system and possibly take complete control of the affected system via a crafted HTTP request.

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-2013-0658
Advisory	http://ics-cert.us-cert.gov/pdf/ICSA-13-043-01.pdf
Risk Assessment	Critical Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to execute arbitrary code on the system.
Affected Products	Schneider Electric Accutech Manager 2.00.1 and earlier
Corero Products	IPS 5500 E-Series and later.
Associated Rule	tln-106604
Associated Rule Set	This rule is automatically enabled in the "Strict 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 2013. All Rights Reserved.