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 Honeywell Tema Remote Installer ActiveX Remote Code Execution Vulnerability.

Issue: The TEMA Remote Installer ActiveX control does not properly validate the origin of an MSI executable before downloading it thereby allowing a remote attacker to install a malicious executable on the victim's machine. This could allow an attacker to execute arbitrary code on the victim's machine by enticing the victim to open a specially crafted website. 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	BID: 50078
Advisory	http://www.us-cert.gov/control_systems/pdf/ICSA-11-285-01.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	EBI R310.1 - TEMA 4.8 EBI R310.1 - TEMA 4.9 EBI R310.1 - TEMA 4.10 EBI R400.2 SP1 - TEMA 5.2 EBI R410.1 - TEMA 5.3.0 EBI R410.2 - TEMA 5.3.1
Corero Products	IPS 5500 E-Series and later.
Associated Rule	tln-025157
Associated Rule Set	This rule is automatically enabled in the "Recommended Client 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