Threat Update Service* Advisory

Protection Pack 2012-08-31-02 Released August 31, 2012

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the Trend Micro Control Manager Cmdprocessor.Exe Buffer Overflow Vulnerability.

Issue: A stack buffer overflow vulnerability exists in the Trend Micro Control Manager. This could allow an attacker to execute arbitrary code on the remote machine by sending a specially crafted packet on TCP port 20101. 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-2011-5001
Vendor Advisory	http://www.trendmicro.com/ftp/documentation/readme/readme_critical_patch_TMCM55_1613.txt
Risk Assessment	Critical Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to gain full control of an unprotected system.
Affected Products	Trend Micro Control Manager 5.5 before Build 1613
Corero Products	IPS 5500 E-Series and later.
Associated Rule	tln-106508
Associated Rule Set	This rule is automatically enabled in the “Recommended Client Protection” and “Recommended Server Protection” rule sets.

* 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