Threat Update Service* Advisory

Protection Pack 2013-04-19-03 Released April 19, 2013

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the McAfee Virtual Technician ActiveX Control Save Insecure Method Vulnerability.

Issue: An arbitrary file upload vulnerability exists in McHealthCheck.dll in McAfee Virtual Technician as it does not properly validate parameters to the Save method. This could allow a remote attacker to upload arbitrary files on the 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-2012-5879
Advisory	https://kc.mcafee.com/corporate/index?page=content&id=SB10040
Risk Assessment	Critical Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to upload arbitrary files to the system.
Affected Products	McAfee Virtual Technician ePO-MVT 6.5.0.2101
Corero Products	IPS 5500 E-Series and later.
Associated Rule	tln-106610
Associated Rule Set	This rule is automatically enabled in the “Strict 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