Threat Update Service* Advisory

Protection Pack 2012-12-06-04 Released December 6, 2012

Purpose: The Corero Security Active Response Team has issued this Prevention Advisory to protect customers against known attacks targeting the VMware OVF Tool Format String Vulnerability.

Issue: A format string vulnerability exists in the VMware OVF Tool. This could allow a remote attacker to execute arbitrary code on the victim's machine by enticing the victim to open a specially crafted OVF 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-2012-3569
Advisory	http://www.vmware.com/security/advisories/VMSA-2012-0015.html
Risk Assessment	Critical Vulnerability
Threat Impact	Remotely exploitable vulnerability that could allow an attacker to gain control of an unprotected system.
Affected Products	VMware OVF Tool 2.1 on Windows, VMware Workstation 8.x before 8.0.5 VMware Player 4.x before 4.0.5
Corero Products	IPS 5500 E-Series and later.
Associated Rule	tln-022162
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