Vulnerability Advisory

Name	VMware Possible Incorrect Permissions On SSL Key Files
VMWare Advisory	http://kb.vmware.com/kb/2467205
Date Released	July 18, 2006
Affected Software	VMware Player for Linux VMware Workstation for Linux VMware Server for Linux VMware ESX Server 2.x VMware Infrastructure 3
Researcher	Nick Breese nick.breese@security-assessment.com

Overview

The configuration program, vmware-config.pl, does not correctly chmod the highly-sensitive generated key file which is used for encrypting traffic for remote administrative connections.

In vmware-config.pl on VMWare Server v1.0 beta (Linux build 24927), lines 6376 - 6382 are meant to chmod the key and certificate files to safe values. However, it does not use the custom safe_chmod() sub-routine which reports errors on failure. Instead, the native Perl chmod() function is used without any return code checking.

```
  # Make key readable only by root (important)
  chmod 0400, shell_string("$certLoc") . '/' . shell_string("$certPrefix")  . '.key';

  # Let anyone read the certificate
  chmod 0444, shell_string("$certLoc") . '/' . shell_string("$certPrefix")  . '.crt';
```

The targets used with the aforementioned chmod() functions are joined together with some parts generated from using a subroutine called shell_string(). This is intended to generate shell representations of string, which is not desired for generating a file path. This causes the target passed to chmod() to be invalid.

Because the safe_chmod() subroutine is not used and no return code checks are performed, the user is not alerted of the chmod() failing.

Depending on the umask set at the time, this could leave the key file readable to any local user on the system.

Exploitation

Exploitation requires local file access on the VMWare product host and appropriate network access. File access could potentially be obtained by manipulating additional existing services. In example, an attacker may be able to leverage required file access via insecure scripts hosted by an HTTP daemon.

Various types of SSL-related attacks can be performed once the key has been obtained.

Solution

Manually change the permissions on the key and certificate to its intended values. The following commands would be appropriate on a default installation:

```
# chmod 400 /etc/vmware/ssl/rui.key
# chmod 444 /etc/vmware/ssl/rui.crt
```

About Security-Assessment.com

Security-Assessment.com is a leader in intrusion testing and security code review, and leads the world with SA-ISO, online ISO17799 compliance management solution. Security-Assessment.com is committed to security research and development, and its team have previously identified a number of vulnerabilities in public and private software vendors products.