

[NEWS] VMware Possible Incorrect Permissions on SSL Key Files

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-07/msg00077.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxxx>
 - *Date:* 26 Jul 2006 15:52:31 +0200
-

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>
-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.
<http://www.securiteam.com/maillinglist.html>

VMware Possible Incorrect Permissions on SSL Key Files

SUMMARY

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.

DETAILS

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';
```

[NEWS] VMware Possible Incorrect Permissions on SSL Key Files

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 a string, which is not desired for generating a file path. This causes the target passed to `chmod()` to be incorrect.

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` being used 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.

Solutions:

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
```

ADDITIONAL INFORMATION

The information has been provided by Nick Breese.

The original article can be found at: <http://kb.vmware.com/kb/2467205>

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

`list-unsubscribe@xxxxxxxxxxxxxx`

In order to subscribe to the mailing list, simply forward this email to: `list-subscribe@xxxxxxxxxxxxxx`

=====
=====

[NEWS] VMware Possible Incorrect Permissions on SSL Key Files

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.