Department of Administration
Enterprise Technology Services

State of Alaska Cyber Security &
Critical Infrastructure Cyber Advisory

June 01, 2009

The following cyber advisory was issued by the State of Alaska and was intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

STATE OF ALASKA ADVISORY NUMBER:
SA2009-029

DATE(S) ISSUED:
06/01/09

Subject:
VMware Security Advisory

Source:
VMWare / MS-ISAC

Systems Affected:

- VMware Workstation 6.5.1 and earlier
- VMware Player 2.5.1 and earlier
- VMware ACE 2.5.1 and earlier
- VMware Server 2.0
- VMware Server 1.0.8 and earlier
- VMware Fusion 2.0.1 and earlier
- VMware ESXi 3.5 without patch ESXe350-200904402-T-BG
- VMware ESX 3.5 without patch ESX350-200904401-BG
- VMware ESX 3.0.3 without patch ESX303-200905401-SG
- VMware ESX 3.0.2 without patch ESX-1008420
- VMware ESX 2.5.5 without update patch 13

Overview:

1. VMware Descheduled Time Accounting driver vulnerability may cause a denial of service in Windows based virtual machines.

- The VMware Descheduled Time Accounting Service is an optional, experimental service that provides improved guest operating system accounting.

  This patch fixes a denial of service vulnerability that could be triggered in a virtual machine by an unprivileged, locally logged-on user in the virtual machine.

  Virtual machines are affected under the following conditions:
  - The virtual machine is running a Windows operating system.
  - The VMware Descheduled Time Accounting driver is installed in the virtual machine. Note that this is an optional (non-default) part of the VMware Tools installation.
  - The VMware Descheduled Time Accounting Service is not running in the virtual machine

  The VMware Descheduled Time Accounting Service is no longer provided in newer versions of VMware Tools, starting with the versions released in Fusion 2.0.2 and ESX 4.0. However, virtual machines migrated from vulnerable releases will still be vulnerable if the three conditions listed above are met, until their tools are upgraded.

  Steps needed to remediate this vulnerability:
  - Guest systems on VMware Workstation, Player, ACE, Server, Fusion:
    - Install the new version of Workstation, Player, ACE, Server, Fusion (see below for version information)
    - Upgrade tools in the virtual machine (virtual machine users will be prompted to upgrade).
  - Guest systems on ESX 3.5, ESXi 3.5, ESX 3.0.2, ESX 3.0.3:
    - Install the relevant patches (see below for patch identifiers)
    - Manually upgrade tools in the virtual machine (virtual machine users will not be prompted to upgrade). Note the VI Client will not show the VMware tools is out of date in the summary tab.
      (Please see http://tinyurl.com/27mpjo page 80 for details.)
  - Guests systems on ESX 4.0 and ESXi 4.0 that have been migrated from ESX 3.5, ESXi 3.5, and ESX 3.0.x:
    - Install/upgrade the new tools in the virtual machine (virtual machine users will be prompted to upgrade)
    - If the Descheduled Time Accounting driver was installed, the tools upgrade will result in an updated driver for Workstation, Player, ACE, Server, ESX 3.0.2, ESX 3.0.3, ESX 3.5, ESXi 3.5. For Fusion, ESX 4.0, and ESXi 4.0 the tools upgrade will result in the removal of the driver.

2. Updated libpng package for the ESX 2.5.5 Service Console
   - The libpng packages contain a library of functions for creating and manipulating PNG (Portable Network Graphics) image format files.
   - A flaw was discovered in libpng that could result in libpng trying to free() random memory if certain, unlikely error conditions occurred. If a carefully-crafted PNG file was loaded by an application linked against libpng, it could cause the application to crash or, potentially, execute arbitrary code with the privileges of the user running the application.

- A flaw was discovered in the way libpng handled PNG images containing "unknown" chunks. If an application linked against libpng attempted to process a malformed, unknown chunk in a malicious PNG image, it could cause the application to crash.
- The VMware version number of libpng after applying the update is libpng-1.0.14-12.i386.rpm.
- The following table lists what action remediates the vulnerability (column 4) if a solution is available:

VMWare Product	***Version***	***Running on (O/S)***	***Patch***
VirtualCenter	Any	Windows	Not affected
Workstation/Server	Any	Any	Not affected
ESXi/ESX	3-4	ESX/ESXi	Not Affected
ESX	2.5.5	ESX	Upgrade Patch 13

Recommendations / Resolution:
Please review the patch/release notes for your product and version:

- VMware Workstation 6.5.2
  - http://www.vmware.com/download/ws/
  - Release notes: http://www.vmware.com/support/ws65/doc/releasenotes_ws652.html
- VMware Player 2.5.2
  - http://www.vmware.com/download/player/
  - Release notes: http://www.vmware.com/support/player25/doc/releasenotes_player252.html
- Windows binary
  - http://download3.vmware.com/software/vmplayer/VMware-player-2.5.2-156735.exe
- Player for Linux (.rpm)
  - http://download3.vmware.com/software/vmplayer/VMware-Player-2.5.2-156735.i386.rpm
- Player for Linux (.tar)
  - http://download3.vmware.com/software/vmplayer/VMware-Player-2.5.2-156735.i386.bundle
- VMware Player 2.5.2 - 64-bit (.rpm)
  - http://download3.vmware.com/software/vmplayer/VMware-Player-2.5.2-156735.x86_64.rpm
- VMware Player 2.5.2 - 64-bit (.bundle)
  - http://download3.vmware.com/software/vmplayer/VMware-Player-2.5.2-156735.x86_64.bundle
- VMware ACE 2.5.2
  - http://www.vmware.com/download/ace/
  - Release notes: http://www.vmware.com/support/ace25/doc/releasenotes_ace252.html
- VMware Server 2.0.1
  - http://www.vmware.com/download/server/
  - Release notes: http://www.vmware.com/support/server2/doc/releasenotes_vmserver201.html
- VMware Server 1.0.9
  - http://www.vmware.com/download/server/
  - Release notes: http://www.vmware.com/support/server/doc/releasenotes_server.html
- VMware Server for Windows 32-bit and 64-bit

    - http://download3.vmware.com/software/vmserver/VMware-server-installer-1.0.9-156507.exe
- VMware Server Windows client package
    - http://download3.vmware.com/software/vmserver/VMware-server-win32-client-1.0.9-156507.zip
- VMware Server for Linux
    - http://download3.vmware.com/software/vmserver/VMware-server-1.0.9-156507.tar.gz
- VMware Server for Linux rpm
    - http://download3.vmware.com/software/vmserver/VMware-server-1.0.9-156507.i386.rpm
- Management Interface
    - http://download3.vmware.com/software/vmserver/VMware-mui-1.0.9-156507.tar.gz
- VMware Server Linux client package
    - http://download3.vmware.com/software/vmserver/VMware-server-linux-client-1.0.9-156507.zip
- VMware Fusion 2.0.4
    - http://www.vmware.com/download/fusion/
- ESXi
    - ESXi 3.5 patch ESXe350-200904401-O-SG (ESXe350-200904402-T-BG)
        - http://download3.vmware.com/software/vi/ESXe350-200904401-O-SG.zip
        - http://kb.vmware.com/kb/1010136
            - NOTES: The three ESXi patches for Firmware "I", VMware Tools "T," and the VI Client "C" are contained in a single offline "O" download file.
- ESX
    - ESX 3.5 patch ESX350-200904401-BG
        - http://download3.vmware.com/software/vi/ESX350-200904401-BG.zip
            - http://kb.vmware.com/kb/1010126
    - ESX 3.0.3 patch ESX303-200905401-SG
        - http://download3.vmware.com/software/vi/ESX303-200905401-SG.zip
            - http://kb.vmware.com/kb/1009940
    - ESX 3.0.2 patch ESX-1008420
        - http://download3.vmware.com/software/vi/ESX-1008420.tgz
            - http://kb.vmware.com/kb/1008420
    - ESX 2.5.5 Upgrade Patch 13
        - http://www.vmware.com/support/esx25/doc/esx-255-200905-patch.html
        - http://download3.vmware.com/software/esx/esx-2.5.5-161312-upgrade.tar.gz

References:

- http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0040
- http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1382
- http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1805
- http://www.vmware.com/security/advisories/VMSA-2009-0007.html