



**State of Alaska Cyber Security &
Critical Infrastructure
Cyber Advisory**

April 6, 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.

ADVISORY NUMBER:

SA2009-021

DATE(S) ISSUED:

4/6/2009

SUBJECT:

Multiple Vulnerabilities in VMware Products

OVERVIEW:

Multiple vulnerabilities have been discovered in several VMware (virtual machine) products that could allow an attacker to gain unauthorized access or take complete control of a vulnerable system. VMware is used to create and run multiple virtual operating systems on a computer. More and more entities are utilizing virtual machines to minimize costs. Depending on the privileges associated with the logged in user or specialized processes, an attacker could exploit these vulnerabilities to install programs; view, change, or delete data; create new accounts with full user rights; or communicate with other systems. Unsuccessful exploitation attempts may cause a denial-of-service condition on all affected systems.

SYSTEMS AFFECTED:

- VMware Workstation 6.5.1 and earlier
- VMware Player 2.5.1 and earlier
- VMware ESXi Server 3.5
- VMware ESX Server 3.5 and earlier
- VMware ACE 2.5.1 and earlier
- VMware Server 2.0
- VMware Server 1.0.8 and earlier
- VMware VirtualCenter
- VMware Fusion 2.x and earlier

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: N/A

DESCRIPTION:

Nine vulnerabilities have been discovered in various VMware applications that could allow attackers to take complete control of or gain unauthorized access to a vulnerable system. VMware applications allow you to create or run virtual machines in a Windows or Linux environment.

Four vulnerabilities may result in denial of service conditions, two vulnerabilities may result in a heap overflow condition, one vulnerability may result in a privilege-escalation issue, one vulnerability may result in an information disclosure, and one vulnerability may create a situation where an unauthorized connection may occur.

Denial of Service

- Two security vulnerabilities in the IOCTL contained in the 'homon.sys' driver, may be exploited by a remote client and may result in a Denial of Service condition.
- A security vulnerability in the 'vmware-authd.exe' may be exploited by a remote client causing a remote denial of service condition.

Privilege Escalation

- A privilege-escalation vulnerability that affects the 'vmci.sys' driver on Workstation, Player, ACE and Server allows an untrusted host to gain elevated privileges, such as permission to read and write local files, or execute local applications.

Unauthorized Access

- An unauthorized access vulnerability in the ACE shared folder would allow an attacker to gain access to disabled shared ACE folders.

Remote Code Execution

- Two security vulnerabilities in the VNnc Codec may be exploited if a user visits a malicious web site or opens a malicious video file. These vulnerabilities could allow a remote attacker to execute arbitrary code on the VMware hosted products. For an attack to be successful the user must be tricked into visiting a malicious web page or opening a malicious video file.

Information Disclosure

- A security vulnerability in VMware ESX allows a remote attacker to obtain a password from the memory in the VirtualCenter Server.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Apply appropriate patches provided by VMware to vulnerable systems immediately after appropriate testing

<http://www.vmware.com/download/>

- Do not visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Apply the Principle of least privilege to all services.
- Ensure that all anti-virus software is up to date with the latest signatures.

REFERENCES:**VMware:**

<http://www.vmware.com/security/advisories/VMSA-2009-0005.html>

Security Focus:

<http://www.securityfocus.com/advisories/16649>

<http://www.securityfocus.com/bid/34373>

SANS:

<http://isc.sans.org/diary.html?storyid=6127>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4916>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3761>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1146>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1147>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0910>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0909>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0908>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0177>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0518>