

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

**April 9, 2010**

*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:**

SA2010-024

**DATE(S) ISSUED:**

4/9/2010

**SUBJECT:**

Multiple Vulnerabilities in VMware Products Could Allow Remote Code Execution

**OVERVIEW:**

Multiple vulnerabilities have been discovered in VMware products that could allow an attacker to gain unauthorized access or take complete control of a vulnerable system. VMware products are used to create and/or run multiple virtual operating systems on a single device. Virtualization is becoming increasingly popular in order to minimize infrastructure costs. Successful exploitation of these vulnerabilities could result in either an attacker gaining the same privileges as the logged on user or specialized processes. Depending on the privileges associated with the user or specialized processes, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploit attempts may result in a denial-of-service condition.

**SYSTEMS AFFECTED:**

- VMware Workstation 7.0 and prior
- VMware VIX API 1.6
- VMware Server 2.0.2 and prior
- VMware Player 3.0 and prior
- VMware Fusion 3.0 and prior
- VMware ESXi Server 4.0 and prior
- VMware ESX Server 4.0 and prior
- VMware ACE 2.6 and prior

**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: High****DESCRIPTION:**

Eight vulnerabilities have been discovered in 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 and/or run virtual machines on a single device. Details of these vulnerabilities follow.

**Remote Code Execution**

A remote arbitrary code-execution vulnerability exists in VMware Tools in the way VMware libraries are referenced. An attacker can exploit this vulnerability by a user opening a malicious file from a network share. The vulnerability can also be exploited on a Windows guest operating systems. This vulnerability affects VMware Workstation, Player, ACE, Server, Fusion, ESX and ESXi.

**Privilege Escalation**

Two privilege-escalation vulnerabilities exist in VMware Tools which can be exploited on Windows host operating systems. This vulnerability may allow a local attacker to execute arbitrary code with the privileges of the logged on user. To exploit this vulnerability an attacker needs to place a malicious executable in a certain location on the guest machine.

The second privilege-escalation vulnerability exists in the USB service on Windows host operating system. To exploit this vulnerability an attacker needs to place a malicious executable in a certain location on the host machine. This vulnerability affects VMware Workstation and Player.

**Heap-Based Buffer Overflow**

Multiple heap-based buffer-overflow vulnerabilities in VMware VMnc Codec may result in an arbitrary code execution. These vulnerabilities can be exploited by a user viewing a malicious webpage or opening a malicious video file. These vulnerabilities affect VMware Workstation, Player, Server and Movie Decoder.

**Format-String**

VMware products are affected by two format-string vulnerabilities. The first format-string vulnerability is in the VMware Remote Console (VMrc) which may result in an arbitrary code execution. This vulnerability can be exploited by a user viewing a malicious webpage or following a malicious URI and affects systems with the VMrc browser plug-in installed.

The second format-string vulnerability is in 'vmrun' may result in an arbitrary code execution. This vulnerability affects VMware VIX API, Workstation, Player, Server and Fusion.

## **Remote Denial-of-Service**

A remote denial-of-service vulnerability affects Windows host operating systems due to an issue in 'vmware-authd'. An attacker can exploit this vulnerability to crash the affected 'authd' service, denying service to legitimate users. This vulnerability affects VMware Workstation, Player, ACE and Server.

## **Information Disclosure**

An information-disclosure vulnerability exists in the virtual networking stack of VMware hosted products. Specifically, a guest operating system could disclose memory of the host system's 'vmware-vmx' process to the virtual network adapter and potentially the network. This vulnerability affects VMware Workstation, Player, ACE, Server and Fusion.

## **RECOMMENDATIONS:**

We recommend the following actions be taken:

- Apply appropriate patches provided by VMware to vulnerable systems immediately after appropriate testing (see <http://downloads.vmware.com/>)
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Apply the Principle of least privilege to all services.

## **REFERENCES:**

### **VMware:**

<http://lists.vmware.com/pipermail/security-announce/2010/000090.html>  
<http://downloads.vmware.com/>

### **Security Focus:**

<http://www.securityfocus.com/bid/39345>

### **Secunia:**

<http://secunia.com/advisories/39206/>  
<http://secunia.com/advisories/36988/>  
<http://secunia.com/advisories/39198/>  
<http://secunia.com/advisories/35346/>  
<http://secunia.com/advisories/39203/>  
<http://secunia.com/advisories/39201/>

### **CVE:**

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1564>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1565>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2042>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3732>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1138>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1139>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1140>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1141>  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1142>