

Enterprise Technology Services



State of Alaska Cyber Security & Critical Infrastructure Cyber Advisory

February 2, 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:

2009-007

DATE(S) ISSUED:

02/02/09

Subject:

VMWare ESX patches address an issue loading corrupt virtual disks and update Service Console packages

Source:

VMWare

Systems Affected:

- VMware ESXi 3.5 without patch ESXe350-200901401-I-SG
- VMware ESX 3.5 without patches ESX350-200901401-SG, ESX350-200901409-SG, ESX350-200901410-SG
- VMware ESX 3.0.3 without patches ESX303-200901405-SG, ESX303-200901406-SG
- VMware ESX 3.0.2 without patches ESX-1007673, ESX-1007674

Overview:

Loading a corrupt delta disk may cause ESX to crash

If the VMDK delta disk of a snapshot is corrupt, an ESX host might crash when the corrupted disk is loaded. VMDK delta files exist for virtual machines with one or more snapshots. This change ensures that a corrupt VMDK delta file cannot be used to crash ESX hosts.

A corrupt VMDK delta disk, or virtual machine would have to be loaded by an administrator.

The following table lists what action remediates the vulnerability (column 4) if a solution is available.

VMWare Product	Product Version	Running on	Replace/patch with
VirtualCenter	Any	Windows	Not affected
Hosted*	Any	Any	Not affected
ESXi	3.5	ESXi	ESXe350-200901401-I-SG
ESX	3.5	ESX	ESX350-200901401-SG
ESX	3.0.3 and below	ESX	Not affected

*hosted products are VMware Workstation, Player, ACE, Server, Fusion.

Updated Service Console package net-snmp

Net-SNMP is an implementation of the Simple Network Management Protocol (SNMP). SNMP is used by network management systems to monitor hosts.

A denial-of-service flaw was found in the way Net-SNMP processes SNMP GETBULK requests. A remote attacker who issued a specially-crafted request could cause the snmpd server to crash.

The Common Vulnerabilities and Exposures Project (cve.mitre.org) has assigned the name CVE-2008-4309 to this issue.

The following table lists what action remediates the vulnerability (column 4) if a solution is available.

VMWare Product	Product Version	Running on	Replace/patch with
VirtualCenter	Any	Windows	Not affected
Hosted*	Any	Any	Not affected
ESXi	3.5	ESXi	Not affected
ESX	3.5	ESX	ESX350-200901401-SG
ESX	3.0.3	ESX	ESX303-200901405-SG
ESX	3.0.2	ESX	ESX-1007673
ESX	2.5.5	ESX	Not affected

*hosted products are VMware Workstation, Player, ACE, Server, Fusion.

Updated Service Console package libxml2

An integer overflow flaw causing a heap-based buffer overflow was found in the libxml2 XML parser. If an application linked against libxml2 processed untrusted, malformed XML content, it could cause the application to crash or, possibly, execute arbitrary code.

A denial of service flaw was discovered in the libxml2 XML parser. If an application linked against libxml2 processed untrusted, malformed XML content, it could cause the application to enter an infinite loop.

VMWare Product	Product Version	Running on	Replace/patch with
VirtualCenter	Any	Windows	Not affected
Hosted*	Any	Any	Not affected
ESXi	3.5	ESXi	Not affected
ESX	3.5	ESX	ESX350-200901410-SG
ESX	3.0.3	ESX	ESX303-200901406-SG
ESX	3.0.2	ESX	ESX-1007674
ESX	2.5.5	ESX	Affected, patch pending

*hosted products are VMware Workstation, Player, ACE, Server, Fusion.

Solution:

Please review the patch/release notes for your product and version and verify the md5sum of your downloaded file.

Patches can be downloaded from:

<http://www.vmware.com/security/advisories/VMSA-2009-0001.html>

References:

CVE numbers

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4914>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4309>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4226>
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4225>

VMWare:

<http://www.vmware.com/security/advisories/VMSA-2009-0001.html>