

# Enterprise Technology Services



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

March 10, 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:**

SA2009-015

### **DATE(S) ISSUED:**

03/10/09

### **Subject:**

Microsoft 03/2009 Security Bulletin Summary

### **Source:**

Microsoft / MS-ISAC

### **Issue 1: Vulnerabilities in Windows Kernel Could Allow Remote Code Execution**

MS09-006 – Critical

#### **Systems Affected:**

- Windows 2000 SP4
- Windows XP SP2 and SP3 (incl. 64 bit)
- Windows Server 2003 SP1 and SP2 (incl 64 bit)
- Windows Vista and SP1 (incl 64 bit)
- Windows Server 2008 (incl 64 bit)

#### **Overview:**

This security update resolves several privately reported vulnerabilities in the Windows kernel. The most serious vulnerability could allow remote code execution if a user viewed a specially crafted EMF or WMF image file from an affected system.

### **Issue 2: Vulnerabilities in DNS and WINS Server Could Allow Spoofing**

MS09-008 – Important

#### **Systems Affected:**

- DNS and WINS servers on:
  - Windows 2000 Server SP4
  - Windows 2003 Server SP1 and SP2
- DNS server on:
  - Windows 2008 Server

#### **Overview:**

This security update resolves two privately reported vulnerabilities and two publicly disclosed vulnerabilities in Windows DNS server and Windows WINS server. These vulnerabilities could allow a remote attacker to redirect network traffic intended for systems on the Internet to the attacker's own systems.

The security update addresses the vulnerabilities by correcting the way that Windows DNS servers cache and validate queries, and by modifying the way that Windows DNS servers and Windows WINS servers handle WPAD and ISATAP registration.

**Recommendations / Resolution:**

Install critical Windows updates via Windows Update or WSUS

**References:**

<http://www.microsoft.com/technet/security/bulletin/MS09-006.msp>

<http://www.microsoft.com/technet/security/bulletin/MS09-008.msp>