



**State of Alaska Cyber Security &
Critical Infrastructure
Cyber Advisory
January 13, 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:

2009-001

DATE(S) ISSUED:

01/13/09

SUBJECT:

Vulnerabilities in Microsoft Server Message Block (SMB) Protocol Could Allow Remote Code Execution

OVERVIEW:

Three remote code execution vulnerabilities exist in the Microsoft Server Message Block (SMB) Protocol. SMB is used mainly to provide shared access to files, printers, serial ports and miscellaneous communications between computers on a local network. Exploitation of these vulnerabilities does not require authentication. Successful exploitation of two of these vulnerabilities could result in an attacker gaining complete control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Successful exploitation of the third vulnerability could result in a Denial of Service (DoS).

Microsoft has released this bulletin to replace MS08-063.

SYSTEMS AFFECTED:

- Windows 2000 Service Pack 4
- Windows XP Service Pack 2 and Service Pack 3
- Windows XP Professional x64 Edition
- Windows XP Professional x64 Edition Service Pack 2
- Windows 2003 Service Pack 1 and Service Pack 2
- Windows Server 2003 x64 Edition
- Windows Server 2003 x64 Edition Service Pack 2
- Windows Server 2003 with SP1 for Itanium-based Systems
- Windows Server 2003 with SP2 for Itanium-based Systems
- Windows Vista

- Windows Vista Service Pack 1
- Windows Vista x64 Edition
- Windows Vista x64 Edition Service Pack 1
- Windows Server 2008 for 32-bit Systems
- Windows Server 2008 for x64-based Systems
- Windows Server 2008 for Itanium-based Systems

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:

Three remote code execution vulnerabilities exist due to insufficient validation of a specially crafted network message using the Microsoft Server Message Block (SMB) Protocol. The three vulnerabilities are:

SMB Buffer Overflow Remote Code Execution Vulnerability
SMB Validation Remote Code Execution Vulnerability
SMB Validation Denial of Service Vulnerability

The vulnerabilities exist in the Server service which is enabled by default in all versions of Windows. Exploitation of these vulnerabilities does not require authentication. Successful exploitation of two of these three vulnerabilities could result in an attacker gaining complete control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Successful exploitation of the third vulnerability could result in a Denial of Service (DoS).

At this time, there are no reports of exploit code being available to the public. However, it should be noted that this vulnerability is likely to be used by Botnets to spread in networks in which only one computer is compromised by other means.

RECOMMENDATIONS:

We recommend the following actions be taken:

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

- Block inbound TCP ports 139 and 445 from the Internet at your network perimeter.
- If you believe you have been affected by targeted attacks exploiting this vulnerability, please follow your organization's policies for incident reporting.

REFERENCES:**Microsoft:**

<http://www.microsoft.com/technet/security/Bulletin/ms09-001.msp>

SANS:

<http://isc.sans.org/diary.html?storyid=5677>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4834>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4835>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4114>

Security Focus:

<http://www.securityfocus.com/bid/33122>