



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

October 15, 2008

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:

2008-021

DATE(S) ISSUED:

10/15/2008

SUBJECT:

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

OVERVIEW:

A remote code execution vulnerability exists 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 network. Successful exploitation will 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.

SYSTEMS AFFECTED:

- Windows 2000
- Windows XP
- Windows 2003
- Windows Vista
- Windows 2008

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:

A remote code execution vulnerability exists due to insufficient validation of specially crafted file names by the Microsoft Server Message Block (SMB) Protocol. To exploit this flaw an attacker must be authenticated on the target system as a legitimate user or as a Guest, and have the target host's IP address, NetBIOS computer name, and SMB port number. In an Active Directory Domain, all users are authenticated to the domain controller and would have all the required information for a successful attack. Successful exploitation will 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.

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.
- Configure your firewall to block inbound SMB traffic from the Internet.
- Disable the Guest account access if it is enabled or preferably, delete the account.

REFERENCES:

Microsoft:

<http://www.microsoft.com/technet/security/Bulletin/MS08-063.msp>

Security Focus:

<http://www.securityfocus.com/bid/31647>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4038>