



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

April 12, 2011

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:

SA2011-017

DATE(S) ISSUED:

4/12/2011

SUBJECT:

Vulnerabilities in SMB Client Could Allow Remote Code Execution (MS11-019)

OVERVIEW:

Two vulnerabilities have been discovered in Microsoft Server Message Block (SMB) Client that could allow for remote code execution. SMB is used to provide shared access to files, printers, serial ports, and other miscellaneous communication between network devices. These vulnerabilities could be exploited if an attacker hosts a website with a specially crafted URI or by sending a specially crafted browser message to the victim machine. Successful exploitation of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user or cause a denial-of-service condition. Depending on the privileges associated with the user, an attacker could then install programs, view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:

- Windows XP
- Windows Vista
- Windows 7
- Windows Server 2003
- Windows Server 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:**

Two vulnerabilities have been discovered in Microsoft Server Message Block (SMB) Client that could allow for remote code execution or cause. These vulnerabilities could be exploited if an attacker hosts a website with a specially crafted URI or by sending a specially crafted browser message to the victim machine. Successful exploitation of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user or cause a denial-of-service condition. Additionally, an attacker on the local network could use a specially crafted Common Internet File System (CIFS) browser message to respond to a legitimate SMB request with a malformed SMB response.

Browser Pool Corruption Vulnerability

Microsoft SMB Client is vulnerable to a memory corruption vulnerability which could allow for remote code execution. This vulnerability exists due to the way the CIFS Browser Protocol implementation improperly parses specially crafted Computer Browser Messages. An attempt to exploit this vulnerability would not require authentication and would allow an attacker to exploit the victim machine by sending a specially crafted browser message.

SMB Client Response Parsing Vulnerability

A remote code execution vulnerability exists in Microsoft SMB Client due to the way it validates specially crafted SMB responses. This vulnerability could be exploited if an attacker hosts a website with a specially crafted URI. If an unsuspecting user clicks this URI it will create a SMB connection with the attacker.

Successful exploitation of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user or cause a denial-of-service condition. Depending on the privileges associated with the user, an attacker could then install programs, view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Implement egress and ingress filtering for TCP ports 139 and 445 at your network perimeter.

REFERENCES:**Microsoft:**

<http://www.microsoft.com/technet/security/bulletin/ms11-019.msp>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0654>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0660>

Securityfocus:#

<http://www.securityfocus.com/bid/46360#>

<http://www.securityfocus.com/bid/47239>