

The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is 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.

DATE(S) ISSUED:

8/10/2010

SUBJECT:

Vulnerabilities in SMB Server Could Allow Remote Code Execution (MS10-054)

OVERVIEW:

Three vulnerabilities have been discovered in Microsoft Server Message Block (SMB) Server that could allow for remote code execution or denial of service. SMB is used to provide shared access to files, printers, serial ports, and other miscellaneous communication between network devices. Successful exploitation of these vulnerabilities could result in an attacker gaining complete control of the affected system or causing denial of service conditions.

SYSTEMS AFFECTED:

Windows XP SP3
Windows Server 2003
Windows Vista
Windows Server 2008
Windows 7

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 vulnerabilities have been discovered in SMB Server that could allow for remote code execution or denial of service conditions.

SMB Pool Overflow Vulnerability

A vulnerability has been discovered in the way SMB Server handles specially crafted SMB packets. An attacker could execute remote code on a vulnerable SMB Server by sending a specially crafted SMB packet designed to exploit this vulnerability. Depending on the version of Windows, authentication may or may not be necessary to exploit this vulnerability. Recent versions of Windows (Vista, Server 2008 and Windows 7) require that an attacker be authenticated unless password-based sharing has been disabled. On Windows XP SP3 or Server 2003 systems, an unauthenticated attacker could exploit this vulnerability. Successful exploitation could allow an attacker to gain the same privileges as the logged on user. 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.

SMB Variable Validation Vulnerability

A variable validation vulnerability has been discovered in SMB Server which could allow for denial of service conditions. An attacker could exploit this vulnerability by sending the SMB Server a specially crafted SMB packet. This will cause the server to stop responding until it is manually restarted.

SMB Stack Exhaustion Vulnerability

A stack exhaustion vulnerability has been discovered in SMB Server which could allow for denial of service conditions. An attacker could exploit this vulnerability by sending the SMB Server a specially crafted SMB compounded request. It is important to note that this vulnerability only affects Server Message Block Version 2 (SMBv2), as compounded requests are not a feature of SMBv1. SMB compound requests are used to package multiple SMBv2 Protocol requests or responses into a single transmission. Successful exploitation will cause the server to stop responding until it is manually restarted.

RECOMMENDATIONS:

The following actions should 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.
- Deploy network intrusion detection systems to monitor network traffic for malicious activity.

REFERENCES:

Microsoft:

<http://www.microsoft.com/technet/security/bulletin/ms10-054.msp>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2550>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2551>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2552>

Security Focus:

<http://www.securityfocus.com/bid/42224>

<http://www.securityfocus.com/bid/42263>

<http://www.securityfocus.com/bid/42267>