

*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:**

2/9/2010

**SUBJECT:**

Vulnerabilities in SMB Server Could Allow Remote Code Execution (MS10-012)

**OVERVIEW:**

Four vulnerabilities have been discovered in Microsoft Server Message Block (SMB) Server that could allow for remote code execution, denial of service, or privilege escalation. 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, causing denial of service conditions, or privilege escalation.

**SYSTEMS AFFECTED:**

Windows 2000  
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:**

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

**SMB Pathname Overflow Vulnerability**

SMB Server is vulnerable to a pathname overflow vulnerability that could allow for remote code execution. An authenticated attacker could execute remote code on a vulnerable SMB Server by

sending a specially crafted SMB packet designed to exploit this vulnerability. When the SMB Server attempts to handle the malicious request, it improperly validates some fields allowing the attacker to take complete control of the system. 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 Memory Corruption Vulnerability**

SMB Server is vulnerable to a memory corruption vulnerability 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 Null Pointer Vulnerability**

SMB Server is vulnerable to a null pointer vulnerability which could allow for denial of service conditions. An attacker could exploit this vulnerability by sending the SMB Server a specially crafted SMB packet. The Server improperly verifies the share and servername fields, resulting in denial of service conditions. This will cause the server to stop responding until it is manually restarted.

### **SMB NTLM Authentication Lack of Entropy Vulnerability**

SMB Server is vulnerable to a NTLM lack of entropy vulnerability which could allow for unauthenticated privilege escalation. This vulnerability is caused by a lack of cryptographic entropy when the SMB server generates challenges to the connecting client. If an attacker incessantly attempts to authenticate against the SMB server, it will generate duplicate values allowing for the attacker to spoof a valid authentication token. The attacker could then upload files, download files, and access SMB network resources masquerading as the logged on user associated with that spoofed token.

### **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/Ms10-012.mspx>

#### **CVE:**

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0020>