

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 SChannel Could Allow Remote Code Execution (MS10-049)

OVERVIEW:

A vulnerability has been discovered in Microsoft SChannel which could allow an attacker to take complete control of a vulnerable system. Microsoft SChannel, or Secure Channel, implements the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols. SSL and TLS are commonly used to implement secure communications for web browsing and other network services. Exploitation may occur if a user visits a web page which is specifically crafted to take advantage of this vulnerability. If successfully exploited, the attacker could gain SYSTEM level privileges and install programs, view, change, or delete data, or create new accounts. Unsuccessful attempts to exploit this vulnerability will likely result in a denial-of-service condition.

Additionally, this Microsoft bulletin (MS10-049) addresses an issue reported in November 2009 which could allow spoofing of TLS/SSL traffic.

SYSTEMS AFFECTED:

Microsoft XP SP3
Microsoft Server 2003

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 SChannel. One vulnerability will allow for remote code execution and one allows for spoofing of communications.

SChannel Malformed Certificate Request Remote Code Execution Vulnerability

The remote code execution vulnerability occurs due to SChannel insufficiently validating certificate request messages. An attacker could exploit the vulnerability by creating a specially crafted webpage. If successfully exploited, the attacker could gain SYSTEM level privileges and install programs, view, change, or delete data, or create new accounts.

TLS/SSL Renegotiation Vulnerability

The spoofing vulnerability is due to a flaw in the TLS protocol that occurs during renegotiation. Successful usage of a man-in-the-middle attack to exploit this issue does not allow for the decryption of

the data, but does allow for the attacker to inject specifically crafted packets in the context of the current session. It should be noted that this vulnerability was originally made public in November of 2009.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.

REFERENCES:

Microsoft:

<http://www.microsoft.com/technet/security/bulletin/ms10-049.msp>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3555>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-2566>

MS-ISAC:

<http://www.msisac.org/advisories/2009/2009-075b.cfm>