

*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:**

10/14/2009

**SUBJECT:**

Vulnerabilities in Windows CryptoAPI Could Allow Spoofing (MS09-056)

**OVERVIEW:**

Two vulnerabilities have been discovered in the Microsoft Windows Cryptographic Application Programming Interface (CryptoAPI). CryptoAPI provides a set of functions included with all Windows products that allows developers to secure Windows applications using cryptography. These vulnerabilities can be exploited to spoof the digital certificates of any web site or application that uses the vulnerable version of the CryptoAPI. Successful exploitation will grant an attacker the ability to spoof digital certificates from a trusted domain or perform man-in-the-middle attacks. The attacker would then be able to impersonate a trusted server and provide users with a false sense of security which could aid in further attacks.

**Please note: Proof of concept code has been published and is publically available. However, we have not received any reports of active exploitation of this vulnerability.**

**SYSTEMS AFFECTED:**

Windows 2000  
Windows XP  
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:**

Two vulnerabilities have been discovered in the Microsoft Windows Cryptographic Application Programming Interface (CryptoAPI) that could allow an attacker to spoof digital certificates. The API fails to properly match the Common Name contained in a digital certificate with the domain providing the certificate. This is due to flaws that occur within the CryptoAPI when parsing ASN.1 data from X.509 certificates.

The first flaw occurs because the CryptoAPI fails to properly handle a unique Object Identifier encoded with Basic Encoding Rules (BER) in an X.509 certificate. If the certificate encoded with BER contains a null terminator, a character with the value zero, the null character will be ruled as superfluous by the API.

The second flaw occurs when the CryptoAPI receives a specially crafted certificate designed to cause an integer overflow. The API does not perform proper error handling for integers that are too large for it to hold, causing them to be parsed incorrectly.

Successful exploitation would grant an attacker the ability to spoof digital certificates from a trusted domain or perform man-in-the-middle attacks. The attacker would then be able to impersonate a trusted server and provide users with a false sense of security which could aid in further attacks.

**Please note: Proof of concept code has been published and is publically available. However, we have not received any reports of active exploitation of this vulnerability.**

#### **RECOMMENDATIONS:**

The following actions should be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.

#### **REFERENCES:**

##### **Microsoft:**

<http://www.microsoft.com/technet/security/Bulletin/MS09-056.mspx>

##### **Security Focus:**

<http://www.securityfocus.com/bid/36577>

##### **IOActive:**

<http://ioactive.com/pdfs/PKILayerCake.pdf>

##### **CVE:**

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2511>