

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:

6/4/2012

SUBJECT:

Unauthorized Digital Certificates Could Allow Spoofing

OVERVIEW:

Microsoft has released information regarding active attacks using unauthorized digital certificates derived from a Microsoft Certificate Authority. Digital certificates are electronic files, issued by organizations known as Certificate Authorities, that provide non-repudiation and enable secure electronic communication between entities on the Internet. An unauthorized certificate could be used to spoof content, perform phishing attacks, or perform man-in-the-middle attacks.

This issue affects all supported releases of Microsoft Windows as well as Windows Mobile and Phone. Please note that there is currently no patch available for Windows Mobile or Phone.

SYSTEMS AFFECTED:

- Windows XP
- Windows Server 2003
- Windows Vista
- Windows Server 2008
- Windows 7
- Windows Mobile 6.x
- Windows Phone 7 & 7.5

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:

Microsoft released information regarding two unauthorized certificates which have been issued by Microsoft and are being used in active attacks. Microsoft identified that an older cryptography algorithm could be exploited and then be used to sign code as if it originated from Microsoft. The issue pertains to their Terminal Services licensing certification authority, which is intended to only be used for license server verification, could also be used to sign any code as Microsoft.

Microsoft has issued an update for all supported releases of Microsoft Windows that addresses the issue. The update revokes the trust of the following intermediate CA certificates:

- Microsoft Enforced Licensing Intermediate PCA (2 certificates)
- Microsoft Enforced Licensing Registration Authority CA (SHA1)

For Windows Mobile 6.x, Windows Phone 7, and Windows Phone 7.5 devices, no update is available at this time.

RECOMMENDATIONS:

The following actions should be taken:

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

REFERENCES:

Microsoft:

<http://technet.microsoft.com/en-us/security/advisory/2718704>

<http://blogs.technet.com/b/srd/>

Security Focus:

<http://www.securityfocus.com/bid/53760>