

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.

SUBJECT: Fraudulent Digital Certificates Could Allow Spoofing

Microsoft has released information which indicates that the DigiCert Sdn. Bhd certification authority has issued 22 certificates with weak 512 bit keys. These weak encryption keys, when broken, could allow an attacker to use the certificates fraudulently to spoof content, perform phishing attacks, or perform man-in-the-middle attacks against all Web browser users.

This issue affects all supported releases of Microsoft Windows.

At this time, there is no indication that any certificates were issued fraudulently. However, these cryptographically weak keys have the potential to allow the certificates to be used in a fraudulent manner.

Microsoft has released an update for all supported versions of Windows that revokes the trust in DigiCert Sdn. Bhd.

Specifically, the update revokes the trust of the following two intermediate CA certificates:

- Digisign Server ID – (Enrich), issued by Entrust.net Certification Authority (2048)
- Digisign Server ID (Enrich), issued by GTE CyberTrust Global Root

RECOMMENDATIONS:

We recommend the following actions be taken:

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

References:

Microsoft

<http://technet.microsoft.com/en-us/security/advisory/2641690>