

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 ISSUED: April 21, 2010

SUBJECT: McAfee False Reports of w32/Wecorl.a Virus

We have received reports from multiple states indicating that they are experiencing what seemed to be an outbreak of the "Wecorl.a" virus. Based on the reports, all systems are running McAfee Anti-Virus, and it is detecting the "Wecorl.a" virus after the recent signature files were updated. The recent McAfee signatures are detecting svchost.exe as being infected with the "wecorl.a" virus. Once detected, the machine continuously reboots itself and may become unusable. It may also cause a Blue screen or DCOM error, followed by shutdown messages after updating to the 5958 DAT on April 21, 2010.

The issue is related to the 5958 DAT file which is causing the false positive. McAfee is currently aware of the false detection issue.

If you have not done so already, do NOT download the 5958 DAT and disable all automatic pull and update tasks.

McAfee has developed an EXTRA.DAT to suppress this detection. This EXTRA.DAT does not fix the issue, it only suppresses the detection.

See <https://kc.mcafee.com/corporate/index?page=content&id=KB68780> for additional information.

Please make sure to subscribe to the McAfee Support Notification Service to receive emails regarding new updates on this detection. You can subscribe by going to [http://my.mcafee.com/content/SNS Subscription Center](http://my.mcafee.com/content/SNS_Subscription_Center)

References:

SANS:

<http://isc.sans.org/diary.html?storyid=8656>

McAfee:

<https://kc.mcafee.com/corporate/index?page=content&id=KB68780>

<http://home.mcafee.com/virusinfo/virusprofile.aspx?key=265240>

<http://community.mcafee.com/thread/24056?start=30&tstart=0>