M E M O R A N D U M

TO: All MDCPS Network Administrators

FROM: Information Technology Services (ITS)

SUBJECT: ***** URGENT *** CRITICAL MICROSOFT WINDOWS UPDATES**

On Tuesday, February 10, Microsoft warned of an extremely serious security vulnerability that appears in all of the current versions of Windows. This vulnerability is capable of causing severe damage if exploited by a worm designed to do so. Details of the vulnerability are covered in Microsoft's Security Bulletin MS04-007. Please refer to the links below:

http://support.microsoft.com/?kbid=828028

http://www.microsoft.com/technet/security/bulletin/ms04-007.asp

The vulnerability, which lies in Microsoft's Corp's ASN.1 (Abstract Syntax Notation 1) library, is among the most serious flaws yet discovered in Windows. Critical core services such as Kerberos, SSL and others can be compromised by this vulnerability. There is no workaround for the vulnerability at this time, but Microsoft has released a patch.

Information Technology Services (ITS) Operational Guidelines

1. The local site tech should leave **ALL** network devices powered on and have them set to receive and apply Operating System Updates automatically.
2. All Sites should be up-to-date in regards to McAfee and EPO updates.
3. Make sure **ALL** target devices have been updated with the current patch.

Specific Directions for this Vulnerability

1. Priority 1 – Patch **ALL** site servers immediately.
2. Priority 2 – Patch all site Win 2003, SP, 2000 and NT desktops.

Even though a worm has not yet appeared, the appearance of a worm designed to exploit this vulnerability, is expected within the very near future. The possible damage that this vulnerability can cause is of such a magnitude that we must act immediately to secure all vulnerable devices.

If a site becomes infected, ITS Network Services will **shut down** the site, thus isolating the contamination and preventing it from spreading to other sites. Shut down may mean **ALL** network traffic (web site, e-mail and mainframe) may need to be blocked. However, in certain cases mainframe traffic will be permitted. In addition, since this e-mail will have been sent out as an early warning, the appropriate ACCESS Center Superintendent will be notified both via telephone and e-mail of all school sites that ITS had to shut down.

As always, your cooperation is greatly appreciated in these matters. If you need assistance with applying the updates or have questions regarding this memo, please call Support Services at 305-995-3705 (0).