April 17, 2006

VULNERABILITY IDENTIFIED WITHIN INTERNET EXPLORER

The FBI has been alerted of a newly discovered vulnerability within Microsoft's Internet Explorer web browser.

The identified vulnerability allows an attacker to spoof the web browser's address bar while displaying web content from another web page. For example, an attacker could be able to display the address bar of a legitimate Web site, while actually displaying a Phishing web page. This vulnerability differs from previous exploits where attackers would overlay the address bar with a .jpg image or re-create the address bar using JavaScript.

Since Microsoft Internet Explorer is a widely used web browser, steps below are being provided to disable active scripting support within the browser in Internet Explorer 6.0:

1. Select Tools from the browser tool bar.
2. Select Internet options.
3. Click on the Security tab and highlight the Internet icon.
4. Click on the Custom Level button.
5. From the drop down menu, select the Scripting section.
6. Click the Disable radio button located underneath the Active Scripting heading.

Disabling scripts should also be used as an interim measure until a patch from Microsoft is available.