COT Security Alert – Critical Microsoft Vulnerability

The Office of the Chief Information Security Officer (OCISO) has been informed by multiple trusted sources that current Microsoft patches address critical vulnerabilities and should be applied as soon as possible after appropriate testing. COT will address this threat on COT-managed devices by expediting the patch schedule. **In addition, users are reminded to use caution in their Internet and email use as described in this notice.**

The expedited patch addresses a total of 49 vulnerabilities. According to the NSA this includes a serious flaw that effects how Microsoft Windows systems validate certificates undermining how Windows verifies the trust between system components. This could allow an attacker to decrypt confidential information gained by performing man-in-the-middle attacks against affected software as well as allowing an attacker to digitally sign a malicious executable. Exploitation of the vulnerability allows attackers to defeat trusted network connections and deliver executable code while appearing as legitimately trusted entities. The vulnerability affects Windows 10 and Windows Server 2016/2019 as well as applications that rely on Windows for trust functionality.

Directives:

- **Administrators** - Apply the appropriate patches or mitigations provided by Microsoft to vulnerable systems immediately after appropriate testing. These are recommended to be completed within 10 days of this notice but system administrators are strongly encouraged to deploy patches as soon as possible.
- **All users** - Run software as a non-privileged user (one without administrative rights) to reduce the effects of a successful attack.
- **All users** - Avoid following links or clicking attachments in emails from unexpected sources.
- **All users** - Use caution while on the Internet and avoid visiting sites that may not be legitimate.

Notice: COT is providing this information so that you are aware of current security threats, vulnerabilities or preventive actions that may affect state government resources. If you suspect you have become victim to a security threat, please contact CommonwealthServiceDesk@ky.gov.

Office of the CISO
Commonwealth Office of Technology
Frankfort, KY 40601
http://technology.ky.gov/CISO/