Microsoft has released 6 security bulletins. Microsoft rates 1 Critical in severity, 4 Important in severity and 1 Moderate in severity.

Microsoft information may be found at the Microsoft Security TechCenter at http://technet.microsoft.com/en-us/security/bulletin/ms12-mar or for each bulletin individually in the links provided below.

MS12-017  **Vulnerability in DNS Server Could Allow Denial of Service (2647170)**  *Important*
http://technet.microsoft.com/en-us/security/bulletin/ms12-017

MS12-018  **Vulnerability in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2641653)**  *Important*

MS12-019  **Vulnerability in DirectWrite Could Allow Denial of Service (2665364)**  *Moderate*

MS12-020  **Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387)**  *Critical*

MS12-021  **Vulnerability in Visual Studio Could Allow Elevation of Privilege (2651019)**  *Important*

MS12-022  **Vulnerability in Expression Design Could Allow Remote Code Execution (2651018)**  *Important*

*Notice*: COT is providing this information so that you are aware of the latest security threats, vulnerabilities, software patches, etc. You should consult with your network administrator or other technical resources to ensure that the appropriate actions for these alerts are followed. If you are a network administrator and need additional information, please call the Help Desk at 502.564.7576.

*Security Administration Branch*
*Commonwealth Office of Technology*
*120 Glenn’s Creek Road, Jones Building*
*Frankfort, KY 40601*
*COTSecurityServicesISS@ky.gov*
*http://technology.ky.gov/CISO/*