Microsoft has released 6 security bulletins. Microsoft rates 4 Critical in severity and 2 Important in severity. Bulletin MS12-027 addresses a flaw which already has a known exploit.

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

**MS12-023** Cumulative Security Update for Internet Explorer (2675157) *Critical*

**MS12-024** Vulnerability in Windows Could Allow Remote Code Execution (2653956) *Critical*

**MS12-025** Vulnerability in .NET Framework Could Allow Remote Code Execution (2671605) *Critical*

**MS12-026** Vulnerabilities in Forefront Unified Access Gateway (UAG) Could Allow Information Disclosure (2663860) *Important*

**MS12-027** Vulnerability in Windows Common Controls Could Allow Remote Code Execution (2664258) *Critical*

**MS12-028** Vulnerability in Microsoft Office Could Allow Remote Code Execution (2639185) *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/