1. HTTP.sys Remote Code Execution Vulnerability
   1. CVE-2015-1635
   2. A vulnerability in Windows Server 2008’s HTTP.sys file could allow remote attackers to execute arbitrary code via specially crafted HTTP requests.
2. Remote Procedure Call vulnerability
   1. CVE-2015-0014
   2. A flaw in Windows server 2008 could allow remote attackers to execute arbitrary code via malformed asynchronous RPC request.
3. ComctL32 Integer Overflow Vulnerability
   1. CVE-2013-3195
   2. A flaw in the DSA\_InsertItem function in the ComctL32.dll in the Windows common control library prevents it from allocating memory correctly, which could in turn allow a remote attacker to execute arbitrary code via a specially crafted value in an argument to an ASP.NET web application.
4. Microsoft Common Use-After-Free vulnerability
   1. CVE-2015-1756
   2. This use-after-free vulnerability in Microsoft Common Controls could allow user-assisted remote attackers to execute arbitrary code via a specially crafted web site accessed with the F12 Developer Tools feature of Internet Explorer.
5. TrueType Font Parsing Vulnerability
   1. CVE-2015-2464
   2. Font Vulnerabilities are a popular way for attackers to gain access to a system, and this particular Windows Server 2008 flaw could allow remote attackers to execute arbitrary code via a specially crafted TrueType font.
6. Remote Desktop Protocol DLL Planting Remote Code Execution Vulnerability
   1. CVE-2015-2473
   2. Windows 2008 Server’s Remote Desktop Protocol (RDP) client contains an untrusted search path vulnerability that could allow local users to gain privileges via a Trojan horse DLL in the current working directory.