2013 年微软发布的正式补丁

目录

微软发布 2013 年 7 月份的安全公告

微软已经发布了 2013 年 7 月份的安全公告，本次公告共 7 个。

1、 MS13-052

.NET Framework 和 Silverlight 中的漏洞可能允许远程执行代码(2861561)

此安全更新可解决 Microsoft .NET Framework 和 Microsoft Silverlight 中五个秘密报告的漏洞和两个公开披露的漏洞。如果受信任的应用程序使用特定代码模式，则这些漏洞中最严重的漏洞可能允许远程执行代码。成功利用此漏洞的攻击者可以获得与登录用户相同的用户权限。那些帐户被配置为拥有较少系统用户权限的用户比具有管理用户权限的用户受到的影响要小。

等级：严重，远程执行代码，可能要求重新启动

受影响的软件：Windows，.NET Framework，Silverlight

http://go.microsoft.com/fwlink/?LinkID=299844

2、 MS13-053

Windows 内核模式驱动程序中的漏洞可能允许远程执行代码(2761226)

此安全更新解决 Microsoft Windows 中两个公开披露的漏洞和六个秘密报告的漏洞。如果用户查看包含特制 TrueType 字体的共享内容，则最严重的漏洞可能允许远程执行代码。成功利用此漏洞的攻击者可以完全控制受影响的系统。

等级：严重，远程执行代码，需要重启动

受影响的软件：Windows

http://go.microsoft.com/fwlink/?LinkID=301423

3、 MS13-054

GDI+中的漏洞可能允许远程执行代码(2848295)

此安全更新可解决 Windows、Office、Lync 和 Visual Studio 中一个秘密报告的漏洞。如果用户查看包含特制 TrueType 字体的共享内容，则该漏洞可能允许远程执行代码。

等级：严重，远程执行代码，可能要求重新启动

受影响的软件：Windows，Office，Visual Studio、Lync

http://go.microsoft.com/fwlink/?LinkId=301531

4、MS13-055

Internet Explorer 累积性安全更新(2846071)

此安全更新可解决 Internet Explorer 中的 17 个秘密报告的漏洞。最严重的漏洞可能在用户使用 Internet Explorer 查看特制网页时允许远程执行代码。成功利用这些最严重的漏洞的攻击者可以获得与当前用户相同的用户权限。那些帐户被配置为拥有较少系统用户权限的用户比具有管理用户权限的用户受到的影响要小。

等级：严重，远程执行代码，需要重启动

受影响的软件：Windows，Internet Explorer

http://go.microsoft.com/fwlink/?LinkID=309324

5、MS13-056

Microsoft DirectShow 中的漏洞可能允许远程执行代码(2845187)

此安全更新可解决 MWindows 中一个秘密报告的漏洞。如果用户打开特制的图像文件，该漏洞可能允许远程执行代码。成功利用此漏洞的攻击者可以获得

与本地用户相同的用户权限。那些帐户被配置为拥有较少系统用户权限的用户比具有管理用户权限的用户受到的影响要小。

等级：严重，远程执行代码，可能要求重新启动

受影响的软件：Windows

http://go.microsoft.com/fwlink/?LinkId=309326

6、MS13-057

Windows Media Format Runtime 中的漏洞可能允许远程执行代码(2847883)

此安全更新可解决 Microsoft Windows 中一个秘密报告的漏洞。如果用户打开特制的媒体文件，该漏洞可能允许远程执行代码。成功利用此漏洞的攻击者可以获得与本地用户相同的用户权限。那些帐户被配置为拥有较少系统用户权限的用户比具有管理用户权限的用户受到的影响要小。

等级：严重，远程执行代码，可能要求重新启动

受影响的软件：Windows

http://go.microsoft.com/fwlink/?LinkId=301528

7、MS13-058

Windows Defender 中的漏洞可能允许特权提升(2847927)

此安全更新可解决适用于 Windows 7 的 Windows Defender 和 Windows Server 2008 R2 上安装的 Windows Defender 中一个秘密报告的漏洞。由于 Windows Defender 所使用的路径名称，该漏洞可能允许特权提升。成功利用此漏洞的攻击者可执行任意代码，并可完全控制受影响的系统。攻击者可随后安装程序;查看、更改或删除数据;或者创建拥有完全用户权限的新帐户。攻击者必须拥有有效的登录凭据才能利用此漏洞。匿名用户无法利用此漏洞。

等级：重要，特权提升，无需重新启动

受影响的软件：Microsoft 安全软件

http://go.microsoft.com/fwlink/?LinkId=308992