2013 年微软发布的正式补丁

目录

微软发布 2013 年 10 月份的安全公告

微软已经发布了 2013 年 10 月份的安全公告，本次公告共 8 个。

1、 MS13-080

Internet Explorer 的累积性安全更新 (2879017)

此安全更新可解决 Internet Explorer 中一个公开披露的漏洞和八个秘密报告的漏洞。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。

http://go.microsoft.com/fwlink/?LinkId=324021

2、 MS13-081

Windows 内核模式驱动程序中的漏洞可能允许远程执行代码 (2870008)

此安全更新可解决 Microsoft Windows 中秘密报告的 7 个漏洞。如果用户查看嵌入 OpenType 或 TrueType 字体文件的共享内容，则这些漏洞中最严重的漏洞可能允许远程执行代码。成功利用这些漏洞的攻击者可以完全控制受影响的系统

http://go.microsoft.com/fwlink/?LinkId=314048

3、 MS13-082

.NET Framework 中的漏洞可能允许远程执行代码 (2878890)

此安全更新可解决 Microsoft .NET Framework 中两个秘密报告的漏洞和一个公开披露的漏洞。如果用户使用能够实例化 XBAP 应用程序的浏览器访问包含特制 OpenType 字体 (OTF) 文件的网站，则最严重的漏洞可能允许远程执行代码。

http://go.microsoft.com/fwlink/?LinkId=318048

4、 MS13-083

Windows 公共控件库中的漏洞可能允许远程执行代码 (2864058)

此安全更新可解决 Microsoft Windows 中一个秘密报告的漏洞。如果攻击者将特制的 Web 请求发送到受影响的系统上运行的 ASP .NET Web 应用程序，该漏洞可能允许远程执行代码。攻击者可能利用此漏洞，无需身份验证即可运行任意代码

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

5、 MS13-084

Microsoft SharePoint Server 中的漏洞可能允许远程执行代码 (2885089)

此安全更新可解决 Microsoft Office 服务器软件中两个秘密报告的漏洞。如果用户在 Microsoft SharePoint Server、Microsoft Office Services 或 Web Apps 的受影响版本中打开特制 Office 文件，则最严重的漏洞可能允许远程执行代码。

http://go.microsoft.com/fwlink/?LinkId=324028

6、 MS13-085

Microsoft Excel 中的漏洞可能允许远程执行代码 (2885080)

此安全更新解决 Microsoft Office 中两个秘密报告的漏洞。如果用户使用受影响的 Microsoft Excel 版本或者其他受影响的 Microsoft Office 软件打开特制的 Office 文件，则这些漏洞可能允许远程执行代码。成功利用该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。

http://go.microsoft.com/fwlink/?LinkId=324026

7、MS13-086

Microsoft Word 中的漏洞可能允许远程执行代码 (2885084)

此安全更新解决 Microsoft Office 中两个秘密报告的漏洞。如果特制文件在 Microsoft Word 的受影响版本或其他受影响的 Microsoft Office 软件中打开，则这些漏洞可能允许远程执行代码。成功利用该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。

http://go.microsoft.com/fwlink/?LinkId=324027

8、MS13-087

Silverlight 中的漏洞可能允许信息泄露 (2890788)

此安全更新解决了 Microsoft Silverlight 中一个秘密报告的漏洞。如果攻击者拥有包含可以利用此漏洞的特制 Silverlight 应用程序的网站，然后诱使用户查看该网站，则该漏洞可能允许信息泄露。攻击者还可能利用受到破坏的网站以及接受或宿主用户提供的内容或广告的网站。此类网站可能包含可以利用此漏洞的特制内容。但是在所有情况下，攻击者无法强制用户访问网站。相反，攻击者必须

诱使用户访问该网站，通常是让用户单击电子邮件或 Instant Messenger 消息中的链接使用户链接到攻击者的网站。它还可能使用横幅广告或其他方式显示特制的 Web 内容，以便将 Web 内容传递至受影响的系统。

http://go.microsoft.com/fwlink/?LinkID=324590