2014 年 11 月微软发布的正式补丁

目录

微软发布 2014 年 11 月份的安全公告

微软已经发布了 2014 年 11 月份的安全公告，本次公告共 15 个。

MS14-064
Windows OLE 中的漏洞可能允许远程执行代码 (3011443)
漏洞描述:

此安全更新可解决 Microsoft Windows 对象链接与嵌入 (OLE) 中 2 个私下报告的漏洞。最严重的漏洞可能在用户使用 Internet Explorer 查看经特殊设计的网页时允许远程执行代码。成功利用这些漏洞的攻击者可以在当前用户的上下文中运行任意代码。如果当前用户使用管理用户权限登录，则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。那些帐户被配置为拥有较少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。
https://technet.microsoft.com/library/security/ms14-064

MS14-065
Internet Explorer 的累积性安全更新 (3003057)
漏洞描述:

此安全更新可解决 Internet Explorer 中的 17 个私下报告的漏洞。最严重的漏洞可能在用户使用 Internet Explorer 查看经特殊设计的网页时允许远程执行代码。成功利用这些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客户比具有管理用户权限的客户受到的影响要小。
https://technet.microsoft.com/library/security/MS14-065

MS14-066
Schannel 中的漏洞可能允许远程执行代码 (2992611)
漏洞描述:

此安全更新可解决 Windows 中的 Microsoft 安全通道 (Schannel) 安全数据包中一个私下报告的漏洞。如果攻击者向 Windows Server 发送特殊设计的数据包，此漏洞可能允许远程执行代码。
https://technet.microsoft.com/library/security/MS14-066

MS14-067
XML Core Services 中的漏洞可能允许远程执行代码 (2993958)
漏洞描述:

此安全更新可解决 Microsoft Windows 中 1 个私下报告的漏洞。如果登录用户访问设计为通过 Internet Explorer 调用 Microsoft XML Core Services (MSXML) 的经特殊设计的网站，该漏

洞可能允许远程执行代码。但是在所有情况下，攻击者都无法强制用户访问此类网站。相反，攻击者必须诱使用户访问一个网站，方法通常是让用户单击电子邮件或 Instant Messenger 请求中的链接以使用户链接到攻击者的网站。
https://technet.microsoft.com/library/security/MS14-067

MS14-068
Kerberos 漏洞可能允许特权提升 (3011780)
漏洞描述:

此安全更新可解决 Microsoft Windows 中 1 个私下报告的漏洞。Kerberos KDC 可能允许攻击者把域用户帐户的权限提升到域管理员帐户级别。攻击者可以利用这些提升权限操作损害任何域中的计算机，包括域控制器。攻击者必须拥有有效的域凭据才能利用此漏洞。受影响的组件可远程使用域凭据标准用户;这不是用户只有本地帐户凭据的情况下。在发布安全公告同时，微软意识到黑土试图利用此漏洞的是非常有限的，仅限于有针对性的攻击。
https://technet.microsoft.com/library/security/MS14-068

MS14-069
Microsoft Office 中的漏洞可能允许远程执行代码 (3009710)
漏洞描述:

此安全更新可解决 Microsoft Office 中 3 个私下报告的漏洞。如果经特殊设计的文件在 Microsoft Office 2007 受影响的版本中打开，则这些漏洞可能允许远程执行代码。成功利用此漏洞的攻击者可能会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客户比具有管理用户权限的客户受到的影响要小。
https://technet.microsoft.com/library/security/MS14-069

MS14-070
TCP/IP 中的漏洞可能允许特权提升 (2989935)
漏洞描述:

此安全更新可解决 TCP/IP 在输入/输出控制 (IOCTL) 过程期间公开报告的漏洞。如果攻击者登录系统并运行经特殊设计的应用程序，则该漏洞可能允许特权提升。成功利用此漏洞的攻击者可以在另一进程的上下文中运行任意代码。如果此进程使用管理员特权运行，则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。
https://technet.microsoft.com/library/security/MS14-070

MS14-071
Windows 音频服务中的漏洞可能允许特权提升 (3005607)
漏洞描述:

此安全更新可解决 Microsoft Windows 中 1 个私下报告的漏洞。如果应用程序使用 Microsoft Windows 音频服务，则该漏洞可能允许特权提升。此漏洞本身不允许运行任意代码。该漏洞必须与允许远程执行代码的另一个漏洞一起使用。
https://technet.microsoft.com/library/security/MS14-071

MS14-072
.NET Framework 中的漏洞可能允许特权提升 (3005210)
漏洞描述:

此安全更新可解决 Microsoft .NET Framework 中的 1 个私下报告的漏洞。如果攻击者向使用 .NET Remoting 的受影响的工作站或服务器发送经特殊设计的数据，则该漏洞可能允许特权提升。只有专门设计为使用 .NET Remoting 的自定义应用程序才会让系统受到该漏洞的攻击。
https://technet.microsoft.com/library/security/MS14-072

MS14-073
Microsoft SharePoint Foundation 中的漏洞可能允许特权提升 (3000431)
漏洞描述:

此安全更新可解决 Microsoft SharePoint Server 中 1 个私下报告的漏洞。成功利用此漏洞的经过身份验证的攻击者可能会在当前 SharePoint 网站上该用户的上下文中运行任意脚本。在基于 Web 的攻击情形中，攻击者可能拥有一个经特殊设计的网站，该网站设计用于利用这些漏洞，然后说服用户浏览此网站。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。这些网站可能包含可以利用这些漏洞的特殊设计的内容。但是在所有情况下，攻击者都无法强制用户查看由攻击者控制的内容。相反，攻击者必须诱使用户采取行动，方法通常是让用户单击电子邮件或 Instant Messenger 中的链接以使用户链接到攻击者的网站，或者让用户打开通过电子邮件发送的附件。
https://technet.microsoft.com/library/security/MS14-073

MS14-074
远程桌面协议中的漏洞可能允许绕过安全功能 (3003743)
漏洞描述:

此安全更新可解决 Microsoft Windows 中 1 个私下报告的漏洞。当远程桌面协议 (RDP) 无法正确记录审核事件时，该漏洞可能允许绕过安全功能。在任何 Windows 操作系统上，RDP 默认为未启用。未启用 RDP 的系统均不存在这一风险。
https://technet.microsoft.com/library/security/MS14-074

MS14-076
IIS 的漏洞可能允许绕过安全功能(2982998)
漏洞描述:

微软此安全更新可解决 Microsoft Internet 信息服务（IIS）中一个秘密报告的漏洞，可能导致“IP 和域限制” 绕过安全功能。成功利用此漏洞可能导致受限制的网络资源可以被受限制或阻止域的客户端访问。
https://technet.microsoft.com/library/security/MS14-076

MS14-077
Active Directory 联合身份验证服务中的漏洞可能允许信息泄露 (3003381)

漏洞描述:

此安全更新可解决 Active Directory 联合身份验证服务 (AD FS) 中 1 个私下报告的漏洞。如果用户从应用程序注销后未关闭其浏览器,攻击者在该用户注销后立即在浏览器中重新打开应用程序，则该漏洞可能允许信息泄露。
https://technet.microsoft.com/library/security/MS14-077

MS14-078
IME（日语）中的漏洞可能允许特权提升 (2992719)
漏洞描述:

此安全更新可解决 Microsoft 输入法编辑器 (IME)（日语）中 1 个私下报告的漏洞。该漏洞可能在安装了 Microsoft IME（日语）的受影响版本的系统上允许基于应用程序沙盒策略执行沙盒逃离。成功利用此漏洞的攻击者可能会逃离容易受到攻击的应用程序的沙盒，并且使用登录用户权限获得受影响的系统的访问权限。如果受影响的系统使用管理权限登录，则攻击者可随后安装程序；查看、更改或删除数据；或者创建拥有完全管理权限的新帐户。
https://technet.microsoft.com/library/security/MS14-078

MS14-079
内核模式驱动程序中的漏洞可能允许拒绝服务 (3002885)
漏洞描述:

此安全更新可解决 Microsoft Windows 中 1 个私下报告的漏洞。如果攻击者在网络共享中放入经特殊设计的 TrueType 字体，随后用户在 Windows Explorer 中导航到此处，则此漏洞可能允许拒绝服务。在基于 Web 的攻击情形中，攻击者可能拥有一个网站，并在上面放置用来利用此漏洞的网页。另外，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可能包含可能利用此漏洞的特殊设计的内容。但是在所有情况下，攻击者都无法强制用户访问此类网站。相反，攻击者必须说服用户访问该网站，方法通常是让用户单击电子邮件或 Instant Messenger 消息中的链接以使用户链接到攻击者的网站。
https://technet.microsoft.com/library/security/MS14-079