2014 年 12 月微软发布的正式补丁

目录

微软发布 2014 年 12 月份的安全公告

微软已经发布了 2014 年 12 月份的安全公告，本次公告共 11 个。

MS14-075

Microsoft Exchange Server 中的漏洞可能允许特权提升 (3009712)

漏洞描述:

此安全更新可解决 Microsoft Exchange Server 中四个私下报告的漏洞。如果用户单击可将用户定向到目标 Outlook Web App 网站经特殊设计的 URL，则最严重的漏洞可能允许特权提升。但是，攻击者无法强迫用户访问这种经特殊设计的网站。相反，攻击者必须诱使用户访问该网站，所采用的方式通常是让用户单击电子邮件或 Instant Messenger 消息中指向攻击者网站的链接，然后诱使他们单击经特殊设计的 URL。

对于 Microsoft Exchange Server 2007、Microsoft Exchange Server 2010 和 Microsoft Exchange Server 2013 的所有受支持版本，此安全更新等级为“重要”。

https://technet.microsoft.com/zh-cn/library/security/MS14-075

MS14-076

Internet Information Services (IIS) 中的漏洞可能允许绕过安全功能 (2982998)

漏洞描述:

此安全更新可解决 Microsoft Internet Information Services (IIS) 中 1 个私下报告的漏洞，此漏洞可能导致绕过“IP 和域限制”安全功能。成功利用此漏洞可能导致来自受限制或被阻止域的客户端拥有访问受限制 Web 资源的权限。

对于 Microsoft Windows 8、Windows 8.1、Windows Server 2012 和 Windows Server 2012 R2 RTM 的所有受支持版本，此安全更新的等级为“重要”。

https://technet.microsoft.com/zh-CN/library/security/ms14-076.aspx

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。

对于以下情况，此安全更新的等级为“重要”:

- 安装在 32 位和基于 x64 版本的 Windows Server 2008 上的 AD FS 2.0
- 安装在基于 x64 版本的 Windows Server 2008 R2 上的 AD FS 2.0
- 安装在基于 x64 版本的 Windows Server 2012 上的 AD FS 2.1
- 安装在基于 x64 版本的 Windows Server 2012 R2 上的 AD FS 3.0

https://technet.microsoft.com/zh-CN/library/security/ms14-077.aspx

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。

在 Windows Server 2003、Windows Vista、Windows Server 2008、Windows 7 和 Windows Server 2008 R2 的所有受支持版本上，此安全更新的等级为“中等”；对于安装了 Microsoft IME（日语）的 Microsoft Office 2007 的所有受支持版本，此安全更新的等级同样为“中等”。

https://technet.microsoft.com/zh-CN/library/security/ms14-078.aspx

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。

对于 Microsoft Windows 所有受支持的版本，此安全更新的等级为“中等”。

https://technet.microsoft.com/zh-CN/library/security/ms14-079.aspx

MS14-080

Internet Explorer 的累积安全更新 (3008923)

漏洞描述:

此安全更新可解决 Internet Explorer 中 14 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。

对于受影响的 Windows 客户端上的 Internet Explorer 6 (IE 6)、Internet Explorer 7 (IE 7)、Internet Explorer 8 (IE 8)、Internet Explorer 9 (IE 9)、Internet Explorer 10 (IE 10) 和 Internet Explorer 11 (IE 11)，此安全更新的等级为“严重”；对于受影响的 Windows 服务器上的 Internet Explorer 6 (IE 6)、Internet Explorer 7 (IE 7)、Internet Explorer 8 (IE 8)、Internet Explorer 9 (IE 9)、Internet Explorer 10 (IE 10) 和 Internet Explorer 11 (IE 11)，此安全更新的等级为“中等”。

https://technet.microsoft.com/zh-CN/library/security/ms14-080.aspx

MS14-081

Microsoft Word 和 Microsoft Office Web App 中的漏洞可能允许远程执行代码 (3017301)

漏洞描述:

此安全更新可解决 Microsoft Word 和 Microsoft Office Web Apps 中两个私下报告的漏洞。如果攻击者说服用户在受影响的 Microsoft Office 软件版本中打开或预览经特制的 Microsoft Word 文件，这两个漏洞可能会允许远程执行代码。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。如果当前用户是以管理用户权限登录，则攻击者随后可以安装程序；查看、更改或删除数据；或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。

对于 Microsoft Word 2007、Microsoft Office 2010、Microsoft Word 2010、Microsoft Word 2013、Microsoft Word 2013 RT、Microsoft Office for Mac 2011、Microsoft Word Viewer、Microsoft Office 兼容包的所有受支持版本以及 Microsoft SharePoint Server 2010、Microsoft SharePoint Server 2013 以及 Microsoft Office Web Apps Server 2013 的受支持版本上受影响的 Microsoft Office 服务和 Web Apps，此安全更新等级为“严重”。

https://technet.microsoft.com/zh-CN/library/security/ms14-081.aspx

MS14-082

Microsoft Office 中的漏洞可能允许远程执行代码 (3017349)

漏洞描述:

此安全更新解决了 Microsoft Office 中一个私下报告的漏洞。如果在受影响的 Microsoft Office 版本中打开经特殊设计的文件，该漏洞可能会允许远程执行代码。成功利用此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。

对于 Microsoft Office 2007、Microsoft Office 2010、Microsoft Office 2013 和 Microsoft Office 2013 RT 的所有受支持版本，此安全更新的等级为“重要”。

https://technet.microsoft.com/zh-CN/library/security/ms14-082.aspx

MS14-083

Microsoft Excel 中的漏洞可能允许远程执行代码 (3017347)

漏洞描述:

此安全更新可解决 Microsoft Excel 中两个私下报告的漏洞。 如果攻击者诱使用户在受影响的 Microsoft Office 软件版本中打开或预览经特殊设计的 Microsoft Excel 文件，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。 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。

对于 Microsoft Excel 2007、Microsoft Excel 2010、Microsoft Excel 2013、Microsoft Excel 2013 RT 和 Microsoft Office 兼容包的所有受支持版本，此安全更新的等级为“重要”。

https://technet.microsoft.com/zh-CN/library/security/ms14-083.aspx

MS14-084

VBScript 脚本引擎中的漏洞可能允许远程执行代码 (3016711)

漏洞描述:

此安全更新可解决 Microsoft Windows 的 VBScript 脚本引擎中一个私下报告的漏洞。 如果用户访问经特殊设计的网站，此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当前用户相同的用户权限。 如果当前用户使用管理用户权限登录，成功利用此漏洞的攻击者便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。

对于受影响的 Windows 客户端上的 VBScript 脚本引擎的受影响版本，此安全更新的等级为“严重”，对于受影响的 Windows 服务器上的 VBScript 脚本引擎的受影响版本，此安全更新的等级为“中等”。

https://technet.microsoft.com/zh-CN/library/security/ms14-084.aspx

MS14-085

Microsoft Graphics 组件中的漏洞可能允许信息泄露 (3013126)

漏洞描述:

此安全更新可解决 Microsoft Windows 中一个公开披露的漏洞。 如果用户浏览包含经特殊设计的 JPEG 内容的网站，该漏洞可能允许信息泄露。 攻击者可能使用该信息泄露漏洞获取有关系统的信息，然后结合其他攻击手段来破坏该系统。 信息泄露漏洞自身不允许执行任意代码。 然而，攻击者可以结合其他漏洞使用该信息泄露漏洞绕过地址空间布局随机化 (ASLR) 等安全功能。

https://technet.microsoft.com/zh-CN/library/security/ms14-085.aspx