2015 年 12 月微软发布的正式补丁

目录

微软发布 2015 年 12 月份的安全公告

微软已经发布了 2015 年 12 月份的安全公告，本次公告共 12 个。

MS15-124

Internet Explorer 累积安全更新 (3116180)

漏洞描述:

此安全更新可解决 Internet Explorer 中的漏洞。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。与拥有管理用户权限的客户相比，帐户被配置为拥有较少系统用户权限的客户受到的影响更小。

对于受影响的 Windows 客户端上的 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 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/ms15-124.aspx

MS15-125

Microsoft Edge 的累积安全更新 (3116184)

漏洞描述:

此安全更新可修复 Microsoft Edge 中的漏洞。最严重的漏洞可能在用户使用 Microsoft Edge 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。与拥有管理用户权限的客户相比，帐户被配置为拥有较少系统用户权限的客户受到的影响更小。

对于 Windows 10 上的 Microsoft Edge 此安全更新的等级为“严重”。

https://technet.microsoft.com/zh-CN/library/security/ms15-125.aspx

MS15-126

用于解决远程执行代码漏洞的 JScript 和 VBScript 累积安全更新 (3116178)

漏洞描述:

此安全更新可解决 Microsoft Windows 的 VBScript 脚本引擎中的漏洞。如果攻击者托管设计为通过 Internet Explorer 利用这些漏洞的经特殊设计的网站（或者会利用接受或托管用户提供的内容火广告的已入侵网站），然后诱骗用户查看网站，则较严重的漏洞可能允许远程执行代码。攻击者也可能在使用 Internet Explorer 呈现引擎将用户定向到经特殊设计的网站的应用程序或 Microsoft Office 文档中嵌入标有“安全初始化”的 ActiveX 控件。

如果当前用户使用管理用户权限登录，则成功利用此漏洞的攻击者可获得与当前用户相同的用户权限，攻击者可以控制受影响的系统。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。

对于受支持版本 Windows Vista、Windows Server 2008 和 Windows Server 2008 R2 的服务器核心安装上 VBScript 脚本引擎受影响的版本，此安全更新等级为“严重”。

https://technet.microsoft.com/zh-CN/library/security/ms15-126.aspx

MS15-127

用于解决远程执行代码漏洞的 Microsoft Windows DNS 安全更新 (3100465)

漏洞描述:

此安全更新修复了 Microsoft Windows 中的一个漏洞。 如果攻击者向 DNS 服务器发送特殊设计的请求，此漏洞可能允许远程执行代码。

对于下列软件，此安全更新的等级为“严重”：Windows Server 2008（32 位系统）的所有受支持版本、Windows Server 2008（基于 x64 的系统）、Windows Server 2008 R2（基于 x64 的系统）、Windows Server 2012 和 Windows Server 2012 R2。

https://technet.microsoft.com/zh-CN/library/security/ms15-127.aspx

MS15-128

用于修复远程执行代码漏洞的 Microsoft 图形组件安全更新程序 (3104503)

漏洞描述:

此安全更新程序修复了 Microsoft Windows、.NET Framework、Microsoft Office、Skype for Business、Microsoft Lync 和 Silverlight 中的多个漏洞。如果用户打开经特殊设计的文档或访问包含经特殊设计的嵌入字体的网页，那么这些漏洞可能允许远程执行代码。

对于以下版本，此安全更新程序的等级为“严重”：

- 所有受支持的 Microsoft Windows 版本
- 所有受支持的 Microsoft Windows 版本上受影响的 Microsoft .NET Framework 版本
- 受影响的 Skype for Business 2016、Microsoft Lync 2013 和 Microsoft Lync 2010 版本
- 受影响的 Microsoft Office 2007 和 Microsoft Office 2010 版本

https://technet.microsoft.com/zh-CN/library/security/ms15-128.aspx

MS15-129

用于修复远程执行代码漏洞的 Silverlight 安全更新程序 (3106614)

漏洞描述:

此安全更新程序修复了 Microsoft Silverlight 中的多个漏洞。如果 Microsoft Silverlight 不正确地处理某些可能导致读写访问冲突的打开和关闭请求，那么这些漏洞中最严重的漏洞可能允许远程执行代码。为了利用此漏洞，攻击者可能会托管一个包含经特殊设计的 Silverlight 应用程序的

网站，然后诱使用户访问遭到入侵的网站。攻击者还可能会利用包含经特殊设计的内容的网站，包括那些接受或托管用户提供的内容或广告的网站。

攻击者无法强迫用户访问遭到入侵的网站。相反，攻击者需要诱使用户执行操作，如单击指向攻击者网站的链接。

对于安装在 Mac 或所有受支持的 Microsoft Windows 版本上的 Microsoft Silverlight 5 和 Microsoft Silverlight 5 Developer Runtime，此安全更新程序的等级为“严重”。

https://technet.microsoft.com/zh-CN/library/security/ms15-129.aspx

MS15-130

用于修复远程执行代码漏洞的 Microsoft Uniscribe 安全更新程序 (3108670)

漏洞描述:

此安全更新程序修复了 Microsoft Windows 中的一个漏洞。如果用户打开经特殊设计的文档或访问包含经特殊设计的字体的不受信任网页，那么此漏洞可能允许远程执行代码。

对于所有受支持的 Windows 7 和 Windows Server 2008 R2 版本，此安全更新程序的等级为“严重”。

https://technet.microsoft.com/zh-CN/library/security/ms15-130.aspx

MS15-131

用于修复远程执行代码漏洞的 Microsoft Office 安全更新程序 (3116111)

漏洞描述:

此安全更新程序修复了 Microsoft Office 中的多个漏洞。如果用户打开经特殊设计的 Microsoft Office 文件，那么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在当前用户的上下文中运行任意代码。与拥有管理用户权限的客户相比，帐户被配置为拥有较少系统用户权限的客户受到的影响更小。

https://technet.microsoft.com/zh-CN/library/security/ms15-131.aspx

MS15-132

用于修复远程执行代码漏洞的 Microsoft Windows 安全更新程序 (3116162)

漏洞描述:

此安全更新程序修复了 Microsoft Windows 中的多个漏洞。如果攻击者访问本地系统并运行经特殊设计的应用程序，那么这些漏洞可能允许远程执行代码。

对于所有受支持的 Microsoft Windows 版本，此安全更新程序的等级为“重要”。

https://technet.microsoft.com/zh-CN/library/security/ms15-132.aspx

MS15-133

用于修复特权提升漏洞的 Windows PGM 安全更新程序 (3116130)

漏洞描述:

此安全更新程序修复了 Microsoft Windows 中的一个漏洞。如果攻击者登录目标系统并通过争用条件运行经特殊设计的应用程序，那么此漏洞可能允许特权提升，从而导致对已经被释放的内存位置的引用。对于易受到攻击的系统，必须安装 Microsoft 消息队列 (MSMQ)，并专门启用 Windows 编程通用多播 (PGM) 协议。MSMQ 在默认配置中不存在；如果已安装，则 PGM 协议可用，但默认处于禁用状态。

对于所有受支持的 Microsoft Windows 版本，此安全更新程序的等级为“重要”。

https://technet.microsoft.com/zh-CN/library/security/ms15-133.aspx

MS15-134

用于解决远程执行代码的 Windows Media Center 安全更新 (3108669)

漏洞描述:

此安全更新可修复 Microsoft Windows 中的漏洞。如果 Windows Media Center 打开引用了恶意代码的经特殊设计的 Media Center 链接 (.mcl) 文件，则其中较为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当前用户相同的用户权限。与拥有管理用户权限的客户相比，帐户被配置为拥有较少系统用户权限的客户受到的影响更小。

对于安装在 Windows Vista、Windows 7、Windows 8 或 Windows 8.1 上 Windows Media Center 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/ms15-134.aspx

MS15-135

用于解决特权提升的 Windows 内核模式驱动程序安全更新 (3119075)

漏洞描述:

此安全更新可修复 Microsoft Windows 中的漏洞。 这些漏洞在攻击者登录目标系统并运行经特殊设计的应用程序时允许特权提升。

对于 Microsoft Windows 的受支持版本，此安全更新的等级为“重要”。

https://technet.microsoft.com/zh-CN/library/security/ms15-135.aspx