2015 年 02 月微软发布的正式补丁

目录

微软发布 2015 年 02 月份的安全公告

微软已经发布了 2015 年 02 月份的安全公告，本次公告共 9 个。

MS15-009

Internet Explorer 安全更新 (3034682)

漏洞描述:

此安全更新可解决 Internet Explorer 中一个公开披露的漏洞和四十个秘密报告的漏洞。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 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/MS15-009

MS15-010

Windows 内核模式驱动程序中的漏洞可能允许远程执行代码 (3036220)

漏洞描述:

此安全更新可修复 Microsoft Windows 中一个公开披露的漏洞和五个秘密报告的漏洞。如果攻击者诱使用户打开特制文档或访问包含嵌入 TrueType 字体的不受信任的网站，则其中最为严重的漏洞可能允许远程执行代码。

对于 Windows 7、Windows Server 2008 R2、Windows 8、Windows Server 2012、Windows RT、Windows 8.1、Windows Server 2012 R2 和 Windows RT 8.1 的所有受支持版本，此安全更新的等级为“严重”；对于 Windows Server 2003、Windows Vista 和 Windows Server 2008 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/ms15-010.aspx

MS15-011

组策略中的漏洞可能允许远程执行代码 (3000483)

漏洞描述:

此安全更新可解决 Microsoft Windows 中一个私下报告的漏洞。如果攻击者诱使用户将配置域的系统连接到受攻击者控制的网络，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完全控制受影响的系统，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 Windows Server 2003、Windows Vista、Windows Server 2008、Windows 7、Windows Server 2008 R2、Windows 8、Windows Server 2012、Windows RT、Windows 8.1、Windows Server 2012 R2 和 Windows RT 8.1 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/ms15-011.aspx

MS15-012

Microsoft Office 中的漏洞可能允许远程代码执行 (3032328)

漏洞描述:

此安全更新可修复 Microsoft Office 中的三个秘密报告的漏洞。如果用户打开经特殊设计的 Microsoft Office 文件，那么这些漏洞可能会允许远程代码执行。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 Microsoft Excel 2007、Microsoft Word 2007、Microsoft Office 2010、Microsoft Excel 2010、Microsoft Word 2010、Microsoft Web Applications 2010、Microsoft Excel 2013、Microsoft Word Viewer、Microsoft Excel Viewer 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/ms15-012.aspx

MS15-013

Microsoft Office 中的漏洞可能允许安全功能规避 (3033857)

漏洞描述:

此安全更新可修复 Microsoft Office 中的一个公开披露的漏洞。如果用户打开经特殊设计的 Microsoft Office 文件，那么此漏洞可能会允许安全功能规避。安全功能规避本身就不允许执行任意代码。不过，攻击者可以结合使用此安全功能规避漏洞和其他漏洞（如远程代码执行漏洞）来运行任意代码。

对于 Microsoft Office 2007、Microsoft Office 2010 和 Microsoft Office 2013 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/ms15-013.aspx

MS15-014

组策略中的漏洞可能允许安全功能规避 (3004361)

漏洞描述:

此安全更新可解决 Microsoft Windows 中一个私下报告的漏洞。如果攻击者通过中间人攻击的方式导致目标系统上的组策略安全配置引擎策略文件遭到损坏或不可读取，则此漏洞可能会允许安全功能规避。这会导致系统上的组策略设置恢复到默认状态，而且安全性也可能会下降。

对于 Microsoft Windows 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/ms15-014.aspx

MS15-015

Microsoft Windows 中的漏洞可能允许特权提升 (3031432)

漏洞描述:

此安全更新可解决 Microsoft Windows 中一个私下报告的漏洞。此漏洞可允许攻击者在进程创建期间利用模拟等级安全检查的缺失来提升特权。成功利用此漏洞的已经过身份验证的攻击者可以获得管理员凭据，并使用这些凭据提升特权。攻击者随后可安装程序；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。

对于 Windows 7、Windows Server 2008 R2、Windows 8、Windows 2012、Windows RT、Windows 8.1、Windows 2012 R2 和 Windows RT 8.1 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/ms15-015.aspx

MS15-016

Microsoft 图形组件中的漏洞可能允许信息泄漏 (3029944)

漏洞描述:

此安全更新可解决 Microsoft Windows 中一个私下报告的漏洞。如果用户浏览的网站中包含经特殊设计的 TIFF 图像，那么此漏洞可能会允许信息泄漏。虽然攻击者无法利用此漏洞来执行代码或直接提升他们的用户权限，但可利用此漏洞获取信息，从而可以使用这些信息尝试进一步入侵受影响的系统。

对于 Microsoft Windows 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/ms15-016.aspx

MS15-017

Virtual Machine Manager 中的漏洞可能允许特权提升 (3035898)

漏洞描述:

此安全更新可修复 Virtual Machine Manager (VMM) 中的一个秘密报告的漏洞。如果攻击者访问受影响的系统，那么此漏洞可能会允许特权提升。攻击者必须拥有有效的 Active Directory 登录凭据，并能够使用这些凭据进行登录才能利用此漏洞。

对于 Microsoft System Center 2012 R2 Virtual Machine Manager 更新汇总 4 和 Microsoft System Center 2012 R2 Virtual Machine Manager 更新汇总 5 预览，此安全更新的等级为“重要”。

https://technet.microsoft.com/zh-CN/library/security/ms15-017.aspx