2015 年 06 月微软发布的正式补丁

目录

微软发布 2015 年 06 月份的安全公告

微软已经发布了 2015 年 06 月份的安全公告，本次公告共 8 个。

MS15-056

Internet Explorer 的累积性安全更新 (3058515)

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 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/library/security/MS15-056

MS15-057

Windows Media Player 中的漏洞可能允许远程执行代码 (3033890)

漏洞描述:

此安全更新可修复 Microsoft Windows 中的漏洞。如果 Windows Media Player 打开恶意网站上经特殊设计的媒体内容，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远程控制受影响的系统。与拥有管理用户权限的用户相比，帐户被配置为拥有较少系统用户权限的用户受到的影响更小。

对于安装到 Windows Server 2003 时的 Windows Media Player 10、安装到 Windows Vista 或 Windows Server 2008 时的 Windows Media Player 11 和安装到 Windows 7 或 Windows Server 2008 R2 时的 Windows Media Player 12，此安全更新的等级为“严重”。

https://technet.microsoft.com/zh-CN/library/security/ms15-057.aspx

MS15-059

Microsoft Office 中的漏洞可能允许远程代码执行 (3064949)

漏洞描述:

此安全更新可修复 Microsoft Office 中的漏洞。最严重的漏洞可能在用户打开经特殊设计的 Microsoft Office 文件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。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。

对于以下所有受支持的软件版本，此安全更新等级为“重要”：

- Microsoft Office 2007
- Microsoft Office 2010
- Microsoft Office 2013
- Microsoft Office 2013 RT

https://technet.microsoft.com/zh-CN/library/security/ms15-059.aspx

MS15-060

Microsoft 常见控件中的漏洞可能允许远程执行代码 (3059317)

漏洞描述:

此安全更新程序可修复 Microsoft Windows 中的一个漏洞。如果用户单击经特殊设计的链接或指向经特殊设计的内容的链接，然后在 Internet Explorer 中调用 F12 开发人员工具，那么此漏洞可能允许远程执行代码。

对于 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，此安全更新程序的等级为“重要”。

https://technet.microsoft.com/zh-CN/library/security/ms15-060.aspx

MS15-061

Windows 内核模式驱动程序中的漏洞可能允许特权提升 (3057839)

漏洞描述:

此安全更新程序可修复 Microsoft Windows 中的多个漏洞。如果攻击者登录系统并运行特制应用程序，最严重的漏洞可能允许特权提升。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 Windows 的所有受支持版本，此安全更新程序的等级为“重要”。

https://technet.microsoft.com/zh-CN/library/security/ms15-061.aspx

MS15-062

Active Directory 联合身份验证服务中的漏洞可能允许特权提升 (3062577)

漏洞描述:

此安全更新程序可修复 Microsoft Active Directory 联合身份验证服务 (AD FS) 中的一个漏洞。如果攻击者将经特殊设计的 URL 提交给目标站点，那么此漏洞可能允许特权提升。在特定情况下，此漏洞会导致经特殊设计的脚本没有得到正确清理，进而可能导致在查看恶意内容的用户的安全性上下文中运行攻击者提供的脚本。对于跨站点脚本攻击，此漏洞需要用户访问被侵站点，才能发生恶意行为。

对于 Active Directory 联合身份验证服务 2.0 和 2.1，此安全更新程序的等级为“重要”。

https://technet.microsoft.com/zh-CN/library/security/ms15-062.aspx

MS15-063

Windows 内核中的漏洞可能允许特权提升 (3063858)

漏洞描述:

此安全更新程序可修复 Microsoft Windows 中的一个漏洞。如果攻击者将恶意 .dll 文件放置在计算机或网络共享上的本地目录中，那么此漏洞可能允许特权提升。攻击者随后需要等待用户运行可以加载恶意 .dll 文件的程序，以便获得特权提升。不过，在任何情况下，攻击者都无法强迫用户访问此类网络共享或网站。

对于 Windows Vista、Windows Server 2008、Windows 7、Windows Server 2008 R2、Windows 8、Windows Server 2012 和 Windows RT 的所有受支持版本，此安全更新程序的等级为“重要”。

https://technet.microsoft.com/zh-CN/library/security/ms15-063.aspx

MS15-064

Microsoft Exchange Server 中的漏洞可能允许特权提升 (3062157)

漏洞描述:

此安全更新程序可修复 Microsoft Exchange Server 中的多个漏洞。如果已经过身份验证的用户单击指向经特殊设计的网页的链接，那么这些漏洞的最严重后果可能是允许特权提升。攻击者无法强迫用户访问此类网站，而是需要诱使用户单击链接，方法通常是诱使用户单击电子邮件或即时消息中的链接。

对于 Microsoft Exchange Server 2013 的所有受支持版本，此安全更新程序的等级为“重要”。

https://technet.microsoft.com/zh-CN/library/security/ms15-064.aspx