2014 年 08 月微软发布的正式补丁

目录

微软发布 2014 年 08 月份的安全公告

微软已经发布了 2014 年 08 月份的安全公告，本次公告共 9 个。

MS14-043

Windows Media Center 中的漏洞可能允许远程执行代码 (2978742)

漏洞描述:

此安全更新可解决 Microsoft Windows 中一个秘密报告的漏洞。如果用户打开可调用 Windows Media Center 资源的特制 Microsoft Office 文件，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。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/zh-CN/library/security/ms14-043.aspx

MS14-044

SQL Server 中的漏洞可能允许特权提升 (2984340)

漏洞描述:

此安全更新可解决 Microsoft SQL Server 中两个秘密报告的漏洞（SQL Server Master Data Services 中一个，SQL Server 关系数据库管理系统中一个）。其中较严重的漏洞影响 SQL Server Master Data Services，如果用户访问会将客户端脚本注入用户的 Internet Explorer 实例中的特制网站，该漏洞可能允许特权提升。在所有情况下，攻击者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 消息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/zh-CN/library/security/ms14-044.aspx

MS14-045

内核模式驱动程序中的漏洞可能允许特权提升 (2984615)

漏洞描述:

此安全更新解决 Microsoft Windows 中三个秘密报告的漏洞。 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。攻击者必须拥有有效的登录凭据并能本地登录才能利用这些漏洞。

https://technet.microsoft.com/zh-CN/library/security/ms14-045.aspx

MS14-046

.NET Framework 中的漏洞可能允许绕过安全功能 (2984625)

漏洞描述:

此安全更新可解决 Microsoft .NET Framework 中的一个秘密报告的漏洞。如果用户访问特制网站，此漏洞可能允许绕过安全功能。在 Web 浏览攻击情形中，成功利用此漏洞的攻击者可能会绕过地址空间布局随机化 (ASLR) 安全功能，它有助于保护用户免遭多种漏洞。该安全功能绕过本身不允许执行任意代码。但是，攻击者可以将此 ASLR 绕过漏洞与另一个漏洞（如远程执行代码漏洞）组合使用，从而利用 ASLR 绕过漏洞来运行任意代码。

https://technet.microsoft.com/zh-CN/library/security/ms14-046.aspx

MS14-047

LRPC 中的漏洞可能允许绕过安全功能 (2978668)

漏洞描述:

此安全更新可解决 Microsoft Windows 中一个秘密报告的漏洞。如果攻击者将此漏洞与另一个漏洞（如远程执行代码漏洞）结合使用，就可以利用 ASLR 绕过漏洞来运行任意代码，那么此漏洞可能允许绕过安全功能。

https://technet.microsoft.com/zh-CN/library/security/ms14-047.aspx

MS14-048

OneNote 中的漏洞可能允许远程执行代码 (2977201)

漏洞描述:

此安全更新可解决 Microsoft OneNote 中一个秘密报告的漏洞。如果特制文件在 Microsoft OneNote 的受影响版本中打开，该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。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/zh-CN/library/security/ms14-048.aspx

MS14-049

Windows Installer 服务中的漏洞可能允许特权提升 (2962490)

漏洞描述:

此安全更新可解决 Microsoft Windows 中一个秘密披露的漏洞。如果攻击者运行特制的应用程序而试图修复以前安装的应用程序，该漏洞可能允许特权提升。攻击者必须拥有有效的登录凭据并能本地登录才能利用此漏洞。

https://technet.microsoft.com/zh-CN/library/security/ms14-049.aspx

MS14-050

Microsoft SharePoint Server 中的漏洞可能允许特权提升 (2977202)

漏洞描述:

此安全更新可解决 Microsoft SharePoint Server 中一个秘密报告的漏洞。经过身份验证的攻击者如果成功利用此漏洞，就可以使用特制的应用程序在当前 SharePoint 网站上该用户的上下文中运行任意 JavaScript。

https://technet.microsoft.com/zh-CN/library/security/ms14-050.aspx

MS14-051

Internet Explorer 的累积性安全更新 (2976627)

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 25 个秘密报告的漏洞。最严重的漏洞可能在用户使用 Internet Explorer 查看特制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/zh-CN/library/security/ms14-051.aspx