2014 年 10 月微软发布的正式补丁

目录

微软发布 2014 年 10 月份的安全公告

微软已经发布了 2014 年 10 月份的安全公告，本次公告共 8 个。

MS14-056
Internet Explorer 的累积性安全更新 (2987107)
漏洞描述:

此安全更新可解决 Internet Explorer 中 14 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/library/security/ms14-056

MS14-057
.NET Framework 中的漏洞可能允许远程执行代码 (3000414)
漏洞描述:

此安全更新可解决 Microsoft .NET Framework 中三个秘密报告的漏洞。如果攻击者将包含国际字符的特制 URI 请求发送到 .NET Web 应用程序，则其中最严重的漏洞可能允许远程执行代码。在 .NET 4.0 应用程序中，容易受到攻击的功能 (iriParsing) 默认情况下被禁用；要利用该漏洞，应用程序必须明确启用此功能。在 .NET 4.5 应用程序中，iriParsing 默认情况下启用，不能被禁用。
https://technet.microsoft.com/library/security/MS14-057

MS14-058
内核模式驱动程序中的漏洞可能允许远程执行代码 (3000061)
漏洞描述:

此安全更新可解决 Microsoft Windows 中两个秘密报告的漏洞。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，则其中较为严重的漏洞可能允许远程执行代码。但是在所有情况下，攻击者无法强制用户执行这些操作。相反，攻击者必须说服用户这样做，方法通常是让用户单击电子邮件或 Instant Messenger 消息中的链接。
https://technet.microsoft.com/library/security/MS14-058

MS14-059
ASP.NET MVC 中的漏洞可能允许绕过安全功能 (2990942)
漏洞描述:

此安全更新解决了 ASP.NET MVC 中一个公开披露的漏洞。如果攻击者诱使用户单击特制链接或

访问包含旨在利用漏洞的特制内容的网页，则此漏洞可能允许绕过安全功能。在基于 Web 的攻击情形中，攻击者可能拥有一个旨在通过 Web 浏览器利用漏洞的特制网站，然后诱使用户查看该网站。攻击者还可能利用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。这些网站可能包含可以利用此漏洞的特制内容。但是在所有情况下，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/library/security/MS14-059

MS14-060

Windows OLE 中的漏洞可能允许远程执行代码 (3000869)

漏洞描述:

此安全更新可解决 Microsoft Windows 中一个秘密报告的漏洞。如果用户打开包含特制 OLE 对象的 Microsoft Office 文件，则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在当前用户的上下文中运行任意代码。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。

https://technet.microsoft.com/library/security/MS14-060

MS14-061

Microsoft Word 和 Office Web Apps 中的漏洞可能允许远程执行代码 (3000434)

漏洞描述:

此安全更新可解决 Microsoft Office 中一个秘密报告的漏洞。如果攻击者诱使用户打开特制 Microsoft Word 文件，此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。

https://technet.microsoft.com/library/security/MS14-061

MS14-062

消息队列服务中的漏洞可能允许特权提升 (2993254)

漏洞描述:

此安全更新可解决 Microsoft Windows 中一个公开披露的漏洞。如果攻击者向消息队列服务发送特制输入/输出控制 (IOCTL) 请求，则该漏洞可能允许特权提升。成功利用此漏洞便可完全访问受影响的系统。默认情况下，消息队列组件不安装在任何受影响的操作系统版本上，而仅由具有管理特权的用户启用。只有手动启用“消息队列服务”组件的客户才可能受此问题的影响。

https://technet.microsoft.com/library/security/MS14-062

MS14-063

FAT32 磁盘分区驱动程序中的漏洞可能允许特权提升 (2998579)

漏洞描述:

此安全更新可解决 Microsoft Windows 中一个秘密报告的漏洞。Windows FASTFAT 系统驱动程序与 FAT32 磁盘分区进行交互的方式中存在一个特权提升漏洞。成功利用此漏洞的攻击者可以使用提升的特权执行任意代码。

https://technet.microsoft.com/library/security/MS14-063