2015 年 4 月微软发布的正式补丁

目录

微软发布 2015 年 4 月份的安全公告

微软已经发布了 2015 年 4 月份的安全公告，本次公告共 11 个。

MS15-032
Internet Explorer 的累积性安全更新 (3038314)
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。
https://technet.microsoft.com/zh-cn/library/security/MS15-032

MS15-033
Microsoft Office 中的漏洞可能允许远程代码执行 (3048019)
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。
https://technet.microsoft.com/zh-cn/library/security/MS15-033

MS15-034
HTTP.sys 中的漏洞可能允许远程执行代码 (3042553)
漏洞描述:

此此安全更新可修复 Microsoft Windows 中的漏洞。 如果攻击者向受影响的 Windows 系统发送经特殊设计的的 HTTP 请求，此漏洞可能允许远程执行代码。
https://technet.microsoft.com/zh-cn/library/security/MS15-034

MS15-035
Microsoft Graphics 组件中的漏洞可能允许远程执行代码 (3046306)
漏洞描述:

此安全更新可修复 Microsoft Windows 中的漏洞。 如果攻击者成功诱使用户浏览经特殊设计的网站、打开经特殊设计的文件或浏览包含经特殊设计的增强型图元文件 (EMF) 图像文件的工作目录，则漏洞可能会允许远程执行代码。 但是在所有情况下，攻击者无法强迫用户执行此类操作；攻击者必须说服用户执行此类操作，通常方式为通过电子邮件或 Instant Messenger 消息

进行诱骗。
https://technet.microsoft.com/zh-cn/library/security/MS15-035

MS15-036
Microsoft SharePoint Server 中的漏洞可能允许特权提升 (3052044)
漏洞描述:

此安全更新可解决 Microsoft Office 服务器和效率软件中的漏洞。 如果攻击者向受影响的 SharePoint server 发送经特殊设计的请求，则该漏洞可能允许特权提升。 成功利用此漏洞的攻击者可以阅读攻击者未授权阅读的内容、使用受害者的身份代表受害者在 SharePoint 网站上执行操作（例如，更改权限和删除内容）以及在受害者的浏览器中注入恶意内容。
https://technet.microsoft.com/zh-cn/library/security/MS15-036

MS15-037
Windows 任务计划程序中的漏洞可能允许特权提升 (3046269)
漏洞描述:

此安全更新可修复 Microsoft Windows 中的漏洞。 成功利用此漏洞的攻击者可以利用已知的无效任务来引发任务计划程序，以在系统帐户的上下文中运行经特殊设计的应用程序。 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。
https://technet.microsoft.com/zh-cn/library/security/MS15-037

MS15-038
Microsoft Windows 中的漏洞可能允许特权提升 (3049576)
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系统并运行特制应用程序时允许提升特权。 要利用这些漏洞，攻击者必须先登录到系统。
https://technet.microsoft.com/zh-cn/library/security/MS15-038

MS15-039
XML Core Services 中的漏洞可能允许绕过安全功能 (3046482)
漏洞描述:

此安全更新可修复 Microsoft Windows 中的漏洞。 如果用户打开经特殊设计的文件，此漏洞可能允许绕过安全功能。 但是在所有情况下，攻击者无法强迫用户打开经特殊设计的文件；攻击者必须说服用户打开此文件，通常方式为通过电子邮件或 Instant Messenger 消息进行诱骗。
https://technet.microsoft.com/zh-cn/library/security/MS15-039

MS15-040
Active Directory 联合身份验证服务中的漏洞可能允许信息泄漏 (3045711)
漏洞描述:

此安全更新可解决 Active Directory 联合身份验证服务 (AD FS) 中的一个漏洞。 如果用户从应用程序注销后未关闭其浏览器，攻击者在该用户注销后立即在浏览器中重新打开应用程序，则该漏洞可能允许信息泄漏。
https://technet.microsoft.com/zh-cn/library/security/MS15-040

MS15-041
.NET Framework 中的漏洞可能允许信息泄漏 (3048010)
漏洞描述:

此安全更新可解决 Microsoft .NET Framework 中的一个漏洞。 如果攻击者向已禁用自定义错误信息的受影响服务器发送经过特殊设计的 Web 请求，则此漏洞可能允许信息泄漏。 成功利用此漏洞的攻击者可以查看部分 web 配置文件，这可能会暴露敏感信息。
https://technet.microsoft.com/zh-cn/library/security/MS15-041

MS15-042
Windows Hyper-V 中的漏洞可能允许拒绝服务 (3047234)
漏洞描述:

此安全更新可修复 Microsoft Windows 中的漏洞。 如果经过身份验证的攻击者在虚拟机 (VM) 会话中运行经特殊设计的应用程序，则此漏洞可能允许拒绝服务。 请注意，拒绝服务不允许攻击者在运行 Hyper-V 主机的其他 VM 上执行代码或提升用户权限，但可能会导致该主机上的其他 VM 在虚拟机管理器中无法管理。
https://technet.microsoft.com/zh-cn/library/security/MS15-042