微软发布 2015 年 08 月份的安全公告

MS15-079

Internet Explorer 的累积安全更新程序 (3082442)
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。

MS15-080

Microsoft Graphics 组件中的漏洞可能允许远程执行代码 (3078662)
此安全更新可修复 Microsoft Windows、Microsoft .NET Framework、Microsoft Office、Microsoft Lync 和 Microsoft Silverlight 中的漏洞。如果用户打开经特殊设计的文档或者访问嵌入了 TrueType 或 OpenType 字体的不受信任网页，则这些漏洞中最严重的漏洞可能允许远程执行代码。

MS15-081

Microsoft Office 中的漏洞可能允许远程执行代码 (3080790)
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。

MS15-082

RDP 中的漏洞可能允许远程执行代码 (3080348)
此安全更新可修复 Microsoft Windows 中的漏洞。如果攻击者先在目标用户的当前工作目录中放置经特殊设计的动态链接库 (DLL) 文件，然后诱使用户打开远程桌面协议 (RDP) 文件或启动旨在加载受信任的 DLL 文件的程序加载攻击者经特殊设计的 DLL 文件，其中最严重的漏洞可能会允许远程执行代码。成功利用这些漏洞的攻击者可以完全控制受影响的系统。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。

MS15-083

服务器消息块中的漏洞可能允许远程执行代码 (3073921)
此安全更新可修复 Microsoft Windows 中的漏洞。如果攻击者向 SMB 服务器错误记录发送特殊设计的数据包，此漏洞可能允许远程执行代码。

MS15-084

XML Core Services 中的漏洞可能允许信息泄露 (3080129)
此安全更新可修复 Microsoft Windows 和 Microsoft Office 中的漏洞。如果用户单击经特殊设计的链接公开内存地址或以显式方式允许使用安全套接字层 (SSL) 2.0，则这些漏洞可能导致信息泄露。但是，在所有情况下，攻击者无法强制用户单击经特殊设计的链接。攻击者必须说服用户单击此链接，通常方式为通过电子邮件或 Instant Messenger 消息进行诱骗。

MS15-085

Mount Manager 中的漏洞可能允许特权提升 (3082487)
此安全更新可修复 Microsoft Windows 中的漏洞。如果攻击者将恶意 USB 设备插入目标系统，则该漏洞可能会允许特权提升。然后，攻击者会将恶意二进制文件写入磁盘并执行。

MS15-086

System Center Operations Manager 中的漏洞可能允许特权提升 (3075158)
此安全更新可解决 Microsoft System Center Configuration Manager 中的一个漏洞。如果用户通过特制 URL 访问受影响的网站，则该漏洞可能允许特权提升。但是，攻击者无法强迫用户访问这样的网站。相反，攻击者必须诱使用户访问该网站，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受影响的网站。

MS15-087

UDDI Services 中的漏洞可能允许特权提升 (3082459)
此安全更新可修复 Microsoft Windows 中的漏洞。如果攻击者通过将恶意

脚本插入网页搜索参数以执行跨站点脚本 (XSS)，则该漏洞可能允许特权提升。用户必须访问随后会在其中执行恶意脚本的经特殊设计的网页。

MS15-088

不安全的命令行参数传递可能会导致信息泄露 (3082458)
此安全更新还有助于解决 Microsoft Windows、Internet Explorer 和 Microsoft Office 中的信息泄露漏洞。为了利用此漏洞，攻击者首先必须使用 Internet Explorer 中的另一个漏洞以在沙盒进程中执行代码。然后，攻击者通过不安全的命令行参数执行 Notepad、Visio、PowerPoint、Excel 或 Word 以引起信息泄露。为了免受此漏洞影响，客户必须应用此公告中提供的更新，以及 MS15-079 中针对 Internet Explorer 提供的更新。同样，运行受影响 Microsoft Office 产品的客户必须还要安装 MS15-081 中提供的适用更新。

MS15-089

WebDAV 中的漏洞可能导致信息泄露 (3076949)
此安全更新可修复 Microsoft Windows 中的漏洞。如果攻击者通过启用了安全套接字层 (SSL) 2.0 的 WebDAV 服务器强制执行加密的 SSL 2.0 会话并使用中间人 (MiTM) 攻击解密部分加密流量，则该漏洞可能导致信息泄露。

MS15-090

Microsoft Windows 中的漏洞可能允许特权提升 (3060716)
此安全更新可修复 Microsoft Windows 中的漏洞。如果攻击者登录受影响系统并运行经特殊设计的应用程序，或说服用户打开经特殊设计的文件以调用容易受攻击的沙盒应用程序，从而允许攻击者逃离沙盒，则该漏洞可能允许特权提升。

MS15-091

Microsoft Edge 的累积安全更新 (3084525)
此安全更新可修复 Microsoft Edge 中的漏洞。最严重的漏洞可能在用户使用 Microsoft Edge 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。

MS15-092

.NET Framework 中的漏洞可能允许特权提升 (3086251)

此安全更新可解决 Microsoft .NET Framework 中的漏洞。如果用户运行经特殊设计的 .NET 应用程序，则该漏洞可能允许特权提升。但是，在所有情况下，攻击者无法强迫用户运行应用程序，攻击者必须说服用户执行此类操作。

MS15-093

Internet Explorer 的安全更新 (3088903)

此安全更新可解决 Internet Explorer 中的漏洞。如果用户使用 Internet Explorer 查看经特殊设计的网页，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。