2011 年微软发布的正式补丁

目录

微软发布 2011 年 1 月份的安全公告

微软已经发布了 2011 年 1 月份的安全公告，本次公告共 2 个，其中包括 1 个严重等级、1 个重要等级。公告中的漏洞涉及的系统包括 windows 系统。

Microsoft 安全公告 MS11-001 - 重要
简要：Windows 备份管理器中的漏洞可能允许远程执行代码 (2478935)
发布日期：一月 11, 2011
漏洞描述：

此安全更新可解决 Windows 备份管理器中一个公开披露的漏洞。 如果用户打开与特制库文件位于同一网络目录下的合法 Windows 备份管理器文件，此漏洞可能允许远程执行代码。 要成功进行攻击，用户必须访问不受信任的远程文件系统位置或 WebDAV 共享，并从该位置打开合法文件，从而可能导致 Windows 备份管理器加载特制的库文件。

对于 Windows Vista 所有受支持的版本，此安全更新等级为“重要”。

此安全更新通过更正 Windows 备份管理器加载外部库的方式来解决此漏洞。

建议：大多数客户均启用了“自动更新”，他们不必采取任何操作，因为此安全更新将自动下载并安装。 尚未启用“自动更新”的客户必须检查更新，并手动安装此更新。

有关详细信息，请参考链接
http://www.microsoft.com/china/technet/security/bulletin/ms11-001.mspx

Microsoft 安全公告 MS11-002 - 严重
简要：Microsoft Data Access Components 中的漏洞可能允许远程执行代码 (2451910)
发布日期：一月 11, 2011
漏洞描述：

此安全更新可解决 Microsoft Data Access Components 中两个秘密报告的漏洞。 如果用户查看特制网页，这些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本地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用户比具有管理用户权限的用户受到的影响要小。

对于 Windows XP、Windows Vista 和 Windows 7 的所有受支持版本，此安全更新的等级为“严重”；对于 Windows Server 2003、Windows Server 2008 和 Windows Server 2008 R2 的所有受支持版本，此安全更新的等级为“重要”。

此安全更新通过确保 MDAC 正确验证字符串长度和内存分配来解决这些漏洞。

建议：大多数客户均启用了“自动更新”，他们不必采取任何操作，因为此安全更新将自动下载并安装。 尚未启用“自动更新”的客户必须检查更新，并手动安装此更新。

有关详细信息，请参考链接
http://www.microsoft.com/china/technet/security/bulletin/ms11-002.mspx

微软发布 2011 年 2 月份的安全公告

微软已经发布了 2011 年 2 月份的安全公告，本次公告共 12 个，其中包括 3 个严重等级、9 个重要等级。公告中的漏洞涉及的系统包括 windows 系统、Office 办公软件。

Microsoft 安全公告 MS11-003 - 严重
简要：Internet Explorer 的累积性安全更新 (2482017)
发布日期：二月 8, 2011
漏洞描述：

此安全更新可解决 Internet Explorer 中两个秘密报告的漏洞和两个公开披露的漏洞。 这些漏洞可在用户使用 Internet Explorer 查看特制 Web 页面或者用户打开一个加载特制库文件的合法 HTML 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获得与本地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用户比具有管理用户权限的用户受到的影响要小。

对于 Windows 客户端上的 Internet Explorer 6、Internet Explorer 7 和 Internet Explorer 8，此安全更新的等级为“严重”；对于 Windows 服务器上的 Internet Explorer 6、Internet Explorer 7 和 Internet Explorer 8，此安全更新的等级为“中等”。

此安全更新通过修改 Internet Explorer 处理内存中对象、处理级联样式表，以及加载外部库的方式来解决这些漏洞。

此安全更新也解决了最初在 Microsoft 安全通报 2488013 中描述的漏洞。

建议：大多数客户均启用了“自动更新”，他们不必采取任何操作，因为此安全更新将自动下载并安装。 尚未启用“自动更新”的客户必须检查更新，并手动安装此更新。

有关详细信息，请参考链接
http://www.microsoft.com/china/technet/security/bulletin/ms11-003.mspx

Microsoft 安全公告 MS11-004 - 重要
简要：Internet Information Services (IIS) FTP 服务中的漏洞可能允许远程执行代码 (2489256)
发布日期：二月 8, 2011
漏洞描述：

此安全更新解决 Microsoft Internet Information Services (IIS) FTP 服务中公开披露的漏洞。 此漏洞允许在 FTP 服务器收到特制 FTP 命令时远程执行代码。 默认情况下不会在 IIS 中安装 FTP 服务。

对于安装在 Windows Vista 和 Windows Server 2008 的所有受支持版本上的用于 IIS 7.0 的 Microsoft FTP Service 7.0 和用于 IIS 7.0 的 Microsoft FTP Service 7.5，对及受支持的所有 Windows 7 和 Windows Server 2008 R2 版本上用于 Internet Information Services 7.5 的 Microsoft FTP Service 7.5，此安全更新等级为“重要”。

此安全更新通过修改 IIS FTP 服务处理特制 FTP 命令的方式来解决此漏洞。

建议：大多数客户均启用了“自动更新”，他们不必采取任何操作，因为此安全更新将自动下载并安装。 尚未启用“自动更新”的客户必须检查更新，并手动安装此更新。

有关详细信息，请参考链接

http://www.microsoft.com/china/technet/security/bulletin/ms11-004.mspx

Microsoft 安全公告 MS11-005 - 重要

简要：Active Directory 中的漏洞可能允许拒绝服务 (2478953)

发布日期：二月 8, 2011

漏洞描述：

此安全更新可解决 Active Directory 中一个公开披露的漏洞。 此漏洞允许在攻击者向受影响的 Active Directory 服务器发送特制数据包时拒绝服务。 攻击者要利用此漏洞，必须在已加入域的计算机上具有有效的本地管理员特权。

对于受支持的所有 Windows Server 2003 版本上的 Active Directory，此安全更新等级为“重要”。

此安全更新通过更正 Active Directory 服务器处理服务主体名称 (SPN) 更新请求的方式解决此漏洞。

建议：大多数客户均启用了“自动更新”，他们不必采取任何操作，因为此安全更新将自动下载并安装。 尚未启用“自动更新”的客户必须检查更新，并手动安装此更新。

有关详细信息，请参考链接

http://www.microsoft.com/china/technet/security/bulletin/ms11-005.mspx

Microsoft 安全公告 MS11-006 - 严重

简要：Windows Shell 图形处理中的漏洞可能允许远程执行代码 (2483185)

发布日期：二月 14, 2011

漏洞描述：

此安全更新解决了 Windows Shell 图形处理器中一个公开披露的漏洞。 如果用户查看特制缩略图，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登录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用户比具有管理用户权限的用户受到的影响要小。对于 Windows XP、Windows Server 2003、Windows Vista 和 Windows Server 2008 的所有受支持版本，此安全更新的等级为“严重”。Windows 7 和 Windows Server 2008 R2 的所有受支持版本不受此漏洞的影响。

此安全更新通过更正 Windows Shell 图形处理器解析缩略图的方式解决此漏洞。

此安全更新也解决了最初在 Microsoft 安全通报 2490606 中描述的漏洞。

建议：大多数客户均启用了“自动更新”，他们不必采取任何操作，因为此安全更新将自动下载并安装。 尚未启用“自动更新”的客户必须检查更新，并手动安装此更新。

有关详细信息，请参考链接

http://www.microsoft.com/china/technet/security/bulletin/ms11-006.mspx

Microsoft 安全公告 MS11-007 - 严重

简要：OpenType Compact 字体格式 (CFF) 驱动程序中的漏洞可能允许远程代码执行 (2485376)

发布日期：二月 8, 2011

漏洞描述：

此安全更新解决了 Windows 的 OpenType Compact 字体格式 (CFF) 驱动程序中一个秘密

报告的漏洞。 如果用户查看用特制 CFF 字体呈现的内容，则该漏洞可能允许远程代码执行。 在所有情况下，攻击者无法强制用户查看特制内容。 相反，攻击者必须蛊惑用户访问该网站，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攻击者的网站。对于 Windows Vista、Windows Server 2008、Windows 7 和 Windows Server 2008 R2 的所有受支持版本，此安全更新的等级为“严重”。对于 Windows XP 和 Windows Server 2003 的所有受支持版本，此安全更新的等级也为“重要”。

此安全更新通过更正 Windows OpenType Compact 字体格式 (CFF) 驱动程序验证特制 OpenType 字体参数值的方式解决该漏洞。

建议：大多数客户均启用了“自动更新”，他们不必采取任何操作，因为此安全更新将自动下载并安装。 尚未启用“自动更新”的客户必须检查更新，并手动安装此更新。

有关详细信息，请参考链接

http://www.microsoft.com/china/technet/security/bulletin/ms11-007.mspx

Microsoft 安全公告 MS11-008 - 重要

简要：Microsoft Visio 中的漏洞可能允许远程执行代码 (2451879)

发布日期：二月 8, 2011

漏洞描述：

此安全更新解决 Microsoft Visio 中两个秘密报告的漏洞。 如果用户打开特制的 Visio 文件，这些漏洞可能允许远程执行代码。 成功利用其中任何一个漏洞的攻击者可以获得与登录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用户比具有管理用户权限的用户受到的影响要小。

对于 Microsoft Office Visio 2002 Service Pack 2、Microsoft Office Visio 2003 Service Pack 3 和 Microsoft Office Visio 2007 Service Pack 2，此安全更新等级为“重要”。

此安全更新通过更正 Microsoft Visio 在解析特制 Visio 文件时处理内存中损坏的结构和对象的方式解决该漏洞。

建议：Microsoft 建议客户尽早应用此更新。

有关详细信息，请参考链接

http://www.microsoft.com/china/technet/security/bulletin/ms11-008.mspx

Microsoft 安全公告 MS11-009 - 重要

简要：JScript 和 VBScript 脚本引擎中的漏洞可能允许信息泄露 (2475792)

发布日期：二月 8, 2011

漏洞描述：

此安全更新解决 JScript 和 VBScript 脚本引擎中的一个秘密报告的漏洞。 该漏洞可在用户访问特制网站时导致信息泄露。 攻击者无法强迫用户访问这些网站。 相反，攻击者必须说服用户访问该网站，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攻击者的网站。

对于 Windows 7 的所有受支持版本，此安全更新的等级为“重要”；对于 Windows Server 2008 R2 的所有受支持版本，此安全更新的等级为“中等”。

此安全更新通过更正 JScript 和 VBScript 脚本引擎处理网页中脚本的方式解决该漏洞。

建议：大多数客户均启用了“自动更新”，他们不必采取任何操作，因为此安全更新将自动下载并安装。 尚未启用“自动更新”的客户必须检查更新，并手动安装此更新。

有关详细信息，请参考链接
http://www.microsoft.com/china/technet/security/bulletin/ms11-009.mspx

Microsoft 安全公告 MS11-010 - 重要
简要：Windows 客户端/服务器运行时子系统中的漏洞可能允许特权提升 (2476687)
发布日期：二月 8, 2011
漏洞描述：

此安全更新解决 Windows XP and Windows Server 2003 中的 Microsoft Windows 客户端/服务器运行时子系统 (CSRSS) 中秘密报告的漏洞。对于这些操作系统的所有受支持版本，此安全更新等级为“重要”。

该漏洞允许在攻击者登录用户的系统并启动在攻击者注销以获取后续用户的登录凭据后继续运行的特制应用程序时发生特权提升。 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。 匿名用户无法利用此漏洞，也无法以远程方式利用此漏洞。

此安全更新通过纠正用户在注销后终止其进程的方式解决该漏洞。

建议：大多数客户均启用了“自动更新”，他们不必采取任何操作，因为此安全更新将自动下载并安装。 尚未启用“自动更新”的客户必须检查更新，并手动安装此更新。

有关详细信息，请参考链接
http://www.microsoft.com/china/technet/security/bulletin/ms11-010.mspx

Microsoft 安全公告 MS11-011 - 重要
简要：Windows 内核中的漏洞可能允许特权提升 (2393802)
发布日期：二月 8, 2011
漏洞描述：

此安全更新解决 Microsoft Windows 中一个公开披露和一个秘密报告的漏洞。 如果攻击者本地登录并运行特制应用程序，这些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。 匿名用户无法利用这些漏洞，也无法以远程方式利用这些漏洞。对于 Microsoft Windows 所有受支持的版本，此安全更新的等级为“重要”。

此安全更新通过确保 Windows 内核在分配内存之前正确验证用户提供的数据解决漏洞。

建议：大多数客户均启用了“自动更新”，他们不必采取任何操作，因为此安全更新将自动下载并安装。 尚未启用“自动更新”的客户必须检查更新，并手动安装此更新。

有关详细信息，请参考链接
http://www.microsoft.com/china/technet/security/bulletin/ms11-011.mspx

Microsoft 安全公告 MS11-012 - 重要
简要：Windows 内核模式驱动程序中的漏洞可能允许特权提升 (2479628)
发布日期：二月 8, 2011
漏洞描述：

此安全更新可解决 Microsoft Windows 中秘密报告的五个漏洞。 如果攻击者本地登录并运行特制应用程序，这些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。 匿名用户无法利用这些漏洞，也无法以远程方式利用这些漏洞。

对于 Microsoft Windows 所有受支持的版本，此安全更新的等级为“重要”。

此安全更新通过更正 Windows 内核模式驱动程序验证从用户模式传递的输入的方式解决此漏洞。

建议：大多数客户均启用了“自动更新”，他们不必采取任何操作，因为此安全更新将自动下载并安装。 尚未启用“自动更新”的客户必须检查更新，并手动安装此更新。

有关详细信息，请参考链接

http://www.microsoft.com/china/technet/security/bulletin/ms11-012.mspx

Microsoft 安全公告 MS11-013 - 重要

简要：Kerberos 中的漏洞可能允许特权提升 (2496930)

发布日期：二月 8, 2011

漏洞描述：

此安全更新可解决 Microsoft Windows 中的一个秘密报告的漏洞和一个公开披露的漏洞。如果通过身份验证的本地攻击者在已加入域的计算机上安装恶意服务，则更加严重的这些漏洞可导致特权提升。

对于 Windows XP、Windows Server 2003、Windows 7 和 Windows Server 2008 R2 的所有受支持版本，此安全更新的等级为“重要”。

此更新通过通过阻止在 Windows Kerberos 和 Windows KDC 中使用弱哈希算法，以及防止客户端将客户端和服务器之间的 Kerberos 通信加密标准降级到 DES 来解决这些漏洞。

建议：大多数客户均启用了“自动更新”，他们不必采取任何操作，因为此安全更新将自动下载并安装。 尚未启用“自动更新”的客户必须检查更新，并手动安装此更新。

有关详细信息，请参考链接

http://www.microsoft.com/china/technet/security/bulletin/ms11-013.mspx

Microsoft 安全公告 MS11-014 - 重要

简要：本地安全机构子系统服务中的漏洞可能允许本地特权提升 (2478960)

发布日期：二月 8, 2011

漏洞描述：

此安全更新可解决 Windows XP 和 Windows Server 2003 中的本地安全授权子系统服务 (LSASS) 中秘密报告的漏洞。对于这些操作系统的所有受支持版本，此安全更新等级为“重要”。

此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。 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。 匿名用户无法利用此漏洞，也无法以远程方式利用此漏洞。

此安全更新通过更正 LSASS 处理身份验证过程中使用的特定值的方式解决该漏洞。

建议：大多数客户均启用了“自动更新”，他们不必采取任何操作，因为此安全更新将自动下载并安装。 尚未启用“自动更新”的客户必须检查更新，并手动安装此更新。

有关详细信息，请参考链接

http://www.microsoft.com/china/technet/security/bulletin/ms11-014.mspx

微软发布 2011 年 3 月份的安全公告

微软已经发布了 2011 年 3 月份的安全公告，本次公告共 3 个，其中包括 1 个严重等级、2 个重要等级。公告中的漏洞涉及的系统包括 windows 系统。

Microsoft 安全公告 MS11-015 - 严重
简要：Windows Media 中的漏洞可能允许远程执行代码 (2510030)
发布日期：三月 16, 2011
漏洞描述：

此安全更新可解决 DirectShow 中一个公开披露的漏洞和 Windows Media Player 与 Windows Media Center 中一个秘密报告的漏洞。如果用户打开特制的 Microsoft Digital Video Recording (.dvr-ms) 文件，其中较严重的漏洞可能允许远程执行代码。 不管怎样，不能强制用户打开文件；攻击要想成功，必须诱使用户这样做。

对于 Windows XP（包括 Windows XP Media Center Edition 2005）的受影响版本；Windows Vista 和 Windows 7 的所有受支持版本；以及 Windows Vista 的 Windows Media Center TV Pack，此安全更新的等级为“严重”。 对于 Windows Server 2008 R2（用于基于 x64 的系统）的所有受支持版本，此安全更新的等级也为“重要”。

此安全更新通过修改库文件和 Windows 媒体文件的打开方式来解决这些漏洞。

建议：大多数客户均启用了“自动更新”，他们不必采取任何操作，因为此安全更新将自动下载并安装。 尚未启用“自动更新”的客户必须检查更新，并手动安装此更新。

有关详细信息，请参考链接
http://www.microsoft.com/china/technet/security/bulletin/ms11-015.mspx

Microsoft 安全公告 MS11-016 - 重要
简要：Microsoft Groove 中的漏洞可能允许远程执行代码 (2494047)
发布日期：三月 8, 2011
漏洞描述：

此安全更新可解决 Microsoft Groove 中一个公开披露的漏洞，如果用户打开与特制库文件位于同一网络目录下的合法 Groove 相关文件，此漏洞可能允许远程执行代码。 那些帐户被配置为拥有较少系统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。

对于 Microsoft Groove 2007 Service Pack 2，此安全更新的等级为“重要”。

此更新通过更正 Microsoft Groove 2007 加载外部库的方式来解决此漏洞。

建议：Microsoft 建议客户尽早应用此更新。

有关详细信息，请参考链接
http://www.microsoft.com/china/technet/security/bulletin/ms11-016.mspx

Microsoft 安全公告 MS11-017 - 重要
简要：远程桌面客户端中的漏洞可能允许远程执行代码 (2508062)
发布日期：三月 9, 2011

漏洞描述：

此安全更新可解决 Windows 远程桌面客户端中一个公开披露的漏洞。 如果用户打开与特制库文件位于同一网络文件夹下的合法远程桌面配置（.rdp）文件，此漏洞可能允许远程执行代码。 要成功进行攻击，用户必须访问不受信任的远程文件系统位置或 WebDAV 共享，并从该位置打开文档，然后由容易受攻击的应用程序加载此文档。

对于 Remote Desktop Connection 5.2 Client、Remote Desktop Connection 6.0 Client、Remote Desktop Connection 6.1 Client 和 Remote Desktop Connection 7.0 Client，此安全更新等级为“重要”。

此安全更新通过更正 Windows 远程桌面客户端加载外部库的方式来解决此漏洞。

建议：大多数客户均启用了“自动更新”，他们不必采取任何操作，因为此安全更新将自动下载并安装。 尚未启用“自动更新”的客户必须检查更新，并手动安装此更新。

有关详细信息，请参考链接

http://www.microsoft.com/china/technet/security/bulletin/ms11-017.mspx