MS13-071：Windows 主题文件中的漏洞可能允许远程执行代码

摘要：此安全更新可解决 Microsoft Windows 中一个秘密报告的漏洞。如果用户在其系统上应用特制的 Windows 主题，则该漏洞可能允许远程执行代码。

版本: 1.0

摘要

此安全更新可解决 Microsoft Windows 中一个秘密报告的漏洞。如果用户在其系统上应用特制的 Windows 主题，则该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或应用主题；要想成功攻击，必须诱使用户这样做。

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。

受影响的软件

操作系统	最大安全影响	综合严重等级	替代的更新
Windows XP			
Windows XP Service Pack 3 (2864063)	远程执行代码	重要	无
Windows XP Professional x64 Edition Service Pack 2 (2864063)	远程执行代码	重要	无
Windows Server 2003			
Windows Server 2003 Service Pack 2 (2864063)	远程执行代码	重要	无
Windows Server 2003 x64 Edition Service Pack 2 (2864063)	远程执行代码	重要	无
Windows Server 2003 SP2（用于基于 Itanium 的系统） (2864063)	远程执行代码	重要	无
Windows Vista			
Windows Vista Service Pack 2 (2864063)	无	没有严重等级[1]	无
Windows Vista x64 Edition Service Pack 2 (2864063)	无	没有严重等级[1]	无

操作系统	最大安全影响	综合严重等级	替代的更新
Windows Server 2008			
Windows Server 2008（用于 32 位系统）Service Pack 2 (2864063)	无	没有严重等级[1]	无
Windows Server 2008（用于基于 x64 的系统）Service Pack 2 (2864063)	无	没有严重等级[1]	无
Windows Server 2008（用于基于 Itanium 的系统）Service Pack 2 (2864063)	无	没有严重等级[1]	无

[1]严重等级不适用于指定软件的此更新，因为本公告中讨论的漏洞的已知攻击媒介已在默认配置中阻止。然而，作为一种纵深防御措施，Microsoft 建议这款软件的客户应用此安全更新。

不受影响的软件

操作系统
Windows 7（用于 32 位系统）Service Pack 1
Windows 7（用于基于 x64 的系统）Service Pack 1
Windows Server 2008 R2（用于基于 x64 的系统）Service Pack 1
Windows Server 2008 R2（用于基于 Itanium 的系统）Service Pack 1
Windows 8（用于 32 位系统）
Windows 8（用于 64 位系统）
Windows Server 2012
Windows RT
Windows 8.1（用于 32 位系统）
Windows 8.1（用于 64 位系统）
Windows Server 2012 R2
Windows RT 8.1
服务器核心安装选项
Windows Server 2008（用于 32 位系统）Service Pack 2（服务器核心安装）
Windows Server 2008（用于基于 x64 的系统）Service Pack 2（服务器核心安装）
Windows Server 2008 R2（用于基于 x64 的系统）Service Pack 1（服务器核心安装）
Windows Server 2012（服务器核心安装）
Windows Server 2012 R2（服务器核心安装）