微软月度信息安全公告
2013年5月

苏鹏
特约讲师

Microsoft | TechNet

议程

- 安全公告
  - MS13-037~MS13-046
- 问与答

2013年5月安全公告概述

- 新发布的安全公告
  - 严重级 MS12-037,038
  - 重要级 MS12-039,040,041,042,043,044,044,045,046

MSRC通告安全等级

- Microsoft Security Response Center (MSRC) 使用严重程度等级来帮助确定漏洞及相关的软件更新紧急性

等级	定义
严重	利用该漏洞可以允许internet蠕虫（例如尼姆达红色代码 冲击波，高波等）无需用户操作就可以传播
重要	利用该漏洞可以危及用户数据的保密性、完整性或者可用性、或者危及资源的完整性或可用性
中等	由于默认配置、审核或难以利用等因素，该漏洞的可利用性比较低
低	利用该漏洞相当困难，或其影响已降至最低

Microsoft 安全公告 MS13-037 - 严重

公告标题	Internet Explorer 的累积性安全更新 (2829530)
受影响软件	对于 Windows 客户端上的 Internet Explorer 6、Internet Explorer 7、Internet Explorer 8、Internet Explorer 9 和 Internet Explorer 10，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、Internet Explorer 8、Internet Explorer 9 和 Internet Explorer 10，此安全更新的等级为“中等”
可能的攻击方式	此安全更新解决 Internet Explorer 中的 11 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
受攻击的影响	远程执行代码

JSON 数组信息泄露漏洞 - CVE-2013-1297

- 一个信息泄露漏洞，可能允许攻击者获得访问和读取 Internet Explorer 中 JSON 数据文件内容的权限。

Microsoft 安全公告 MS13-038 – 严重

公告标题	HTTP.sys 中的漏洞可能允许拒绝服务 (2829254)
受影响软件	对于 Windows 8 和 Windows Server 2012 的所有受支持版本，此安全更新等级为“重要”
可能的攻击方式	此安全更新可解决 Microsoft Windows 中一个秘密报告的漏洞。如果攻击者向受影响的 Windows 服务器或客户端发送特制 HTTP 数据包，该漏洞可能允许拒绝服务。
受攻击的影响	拒绝服务

HTTP.sys 拒绝服务漏洞 - CVE-2013-1305

- 当 HTTP 协议堆栈 (HTTP.sys) 不正确地处理恶意 HTTP 标头时，Windows Server 2012 和 Windows 8 中存在一个拒绝服务漏洞。成功利用此漏洞的攻击者可能通过向受影响的 Windows 服务器或客户端发送特制 HTTP 标头来在 HTTP 协议堆栈中触发一个无限循环。

Microsoft 安全公告 MS13-039 – 重要

公告标题	HTTP.sys 中的漏洞可能允许拒绝服务 (2829254)
受影响软件	对于 Microsoft SharePoint Server 2013 的所有受支持版本，此安全更新等级为“重要”
可能的攻击方式	此安全更新解决了 Microsoft SharePoint Server 中一个公开披露的漏洞。
受攻击的影响	信息泄露

不正确的访问权限信息泄露漏洞 - CVE-2013-1290

- SharePoint Server 对特定 SharePoint 列表强制使用访问控件的方式中存在一个信息泄露漏洞。

Microsoft 安全公告 MS13-040 – 重要

公告标题	.NET Framework 中的漏洞可能允许欺骗 (2836440)
受影响软件	对于 Microsoft Windows 所有受影响版本上的 Microsoft .NET Framework 2.0 Service Pack 2、Microsoft .NET Framework 3.5、Microsoft .NET Framework 3.5.1、Microsoft .NET Framework 4 和 Microsoft .NET Framework 4.5，此安全更新的等级为“严重”。
可能的攻击方式	此安全更新可解决 .NET Framework 中的一个秘密报告的漏洞和一个公开披露的漏洞 。如果 .NET 应用程序收到特制 XML 文件，则最严重的漏洞可能允许欺骗。
受攻击的影响	欺骗

XML 数字签名欺骗漏洞 - CVE-2013-1336

- 如果 Windows 内核不正确地处理内存中的对象，则存在一个特权提升漏洞。成功利用此漏洞的攻击者可以获得更高的特权和读取任意多次内核内存。

身份验证绕过漏洞 - CVE-2013-1337

- 当设置自定义 WCF 终结点身份验证时，Microsoft .NET Framework 不正确地创建身份验证策略要求的方式中存在一个安全功能绕过漏洞。

Microsoft 安全公告 MS13-041 – 重要

公告标题	DjVuLibre 中的漏洞可能允许远程执行代码 (2834695)
受影响软件	对于 Microsoft Communicator 2007 R2、Microsoft Lync 2010、Microsoft Lync 2010 Attendee 和 Microsoft Lync Server 2013 的受支持版本，此安全更新的等级为“重要”
可能的攻击方式	此安全更新可解决 Microsoft Lync 中一个秘密报告的漏洞。如果攻击者在 Lync 或 Communicator 中演示时共享特制内容（例如文件或程序），然后诱使用户接受邀请以查看或共享可演示的内容，则该漏洞可能允许远程执行代码
受攻击的影响	远程执行代码

Lync RCE 漏洞 - CVE-2013-1302

- 当 Lync 控件尝试访问内存中已被删除的对象时，存在一个远程执行代码漏洞。攻击者可以通过诱使目标用户接受邀请以在 Lync 或 Communicator 会话内启动特制内容来利用此漏洞。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。

Microsoft 安全公告 MS13-042 – 重要

公告标题	**Microsoft Publisher 中的漏洞可能允许远程执行代码 (2830397)**
受影响软件	对于 Microsoft Publisher 2003、Microsoft Publisher 2007 和 Microsoft Publisher 2010 的受支持版本，此安全更新的等级为“重要”。
可能的攻击方式	此安全更新可解决 Microsoft Office 中 11 个秘密报告的漏洞。如果用户使用受影响的 Microsoft Publisher 版本打开特制的 Publisher 文件，则这两个漏洞可能允许远程执行代码
受攻击的影响	远程执行代码

多个 Microsoft Publisher 远程执行代码漏洞

CVE 编号	漏洞标题	当 Publisher 执行以下操作时存在漏洞…
CVE-2013-1316	Publisher 负值分配漏洞	…分析特制 Publisher 文件时不正确地验证阵列大小。
CVE-2013-1317	Publisher 整数溢出漏洞	…尝试确定分配的大小，从而导致整数溢出情形。
CVE-2013-1318	Publisher 损坏界面指针漏洞	…分析特制 Publisher 文件时不正确地使用已损坏指针。
CVE-2013-1319	Publisher 返回值处理漏洞	…分析特制 Publisher 文件时忽略返回的方法值。
CVE-2013-1320	Publisher 缓冲区溢出漏洞	…分析特制 Publisher 文件时将不正确的字节数读取到阵列中。
CVE-2013-1321	Publisher 返回值验证漏洞	…分析特制 Publisher 文件时无法正确地验证返回的值类型。
CVE-2013-1322	Publisher 无效的范围检查漏洞	…分析特制 Publisher 文件时验证表范围数据。
CVE-2013-1323	Publisher 不正确的空值处理漏洞	…分析特制 Publisher 文件时不正确地处理空值。
CVE-2013-1327	Publisher 签名整数漏洞	…分析特制 Publisher 文件期间分配内存时无法出现经过签名的值。
CVE-2013-1328	Publisher 指针处理漏洞	…处理特制 Publisher 文件时无法正确验证指针。
CVE-2013-1329	Publisher 缓冲区下溢漏洞	…分析特制 Publisher 文件时允许将负数传入到字节阵列插入中。

Microsoft 安全公告 MS13-043 – 重要

公告标题	Microsoft Word 中的漏洞可能允许远程执行代码 (2830399)
受影响软件	对于 Microsoft Word 2003 和 Microsoft Word Viewer 的所有受支持版本，此安全更新等级为“重要”
可能的攻击方式	此安全更新可解决 Microsoft Office 中一个秘密报告的漏洞。如果用户打开特制文件或在受影响的 Microsoft Office 软件版本中预览特制的电子邮件，则该漏洞可能允许远程执行代码
受攻击的影响	远程执行代码

Word 形状损坏漏洞 - CVE-2013-1335

- Microsoft Word 分析 Word 文件中的内容的方式中存在一个远程执行代码漏洞。成功利用此漏洞的攻击者可以完全控制受影响的系统。

Microsoft 安全公告 MS13-044 – 重要

公告标题	Microsoft Visio 中的漏洞可能允许信息泄露 (2834692)
受影响软件	对于 Microsoft Visio 2003、Microsoft Visio 2007 和 Microsoft Visio 2010 的所有受支持版本，此安全更新的等级为“重要”
可能的攻击方式	此安全更新解决了 Microsoft Office 中一个秘密报告的漏洞。如果用户打开特制的 Visio 文件，则该漏洞可能允许信息泄露。
受攻击的影响	信息泄露

XML 外部实体解析漏洞 - CVE-2013-1301

- Microsoft Visio 分析包含外部实体的特制 XML 文件的方式中存在一个信息泄露漏洞。

Microsoft 安全公告 MS13-045 – 重要

公告标题	Windows 软件包中的漏洞可能导致信息泄露 (2813707)
受影响软件	对于安装在 Microsoft Windows 的所有受支持版本上的 Windows Writer，此安全更新的等级为“重要”
可能的攻击方式	此安全更新可解决 Windows 软件包中一个秘密报告的漏洞。如果用户使用特制 URL 打开 Windows Writer，则该漏洞可能允许信息泄露。成功利用此漏洞的攻击者可能会替代 Windows Writer 代理设置并覆盖目标系统上用户可以访问的文件
受攻击的影响	信息泄露

Windows 软件包不正确 URI 处理漏洞 - CVE-2013-0096

- 当 Windows Writer 无法正确处理特制 URL 时，存在一个信息泄露漏洞。成功利用此漏洞的攻击者可能会替代 Windows Writer 代理设置并覆盖目标系统上用户可以访问的文件。

Microsoft 安全公告 MS13-046 – 重要

公告标题	内核模式驱动程序中的漏洞可能允许特权提升 (2840221)
受影响软件	对于 Windows XP、Windows Vista、Windows Server 2008、Windows 7、Windows Server 2008 R2、Windows 8、Windows Server 2012 和 Windows RT 的所有受支持版本
可能的攻击方式	此安全更新解决 Microsoft Windows 中三个秘密报告的漏洞。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。
受攻击的影响	特权提升

DirectX 图形内核子系统双重提取漏洞 - CVE-2013-1332

- 当 Microsoft DirectX 图形内核子系统 (dxgkrnl.sys) 不正确地处理内存中的对象时，存在一个特权提升漏洞。

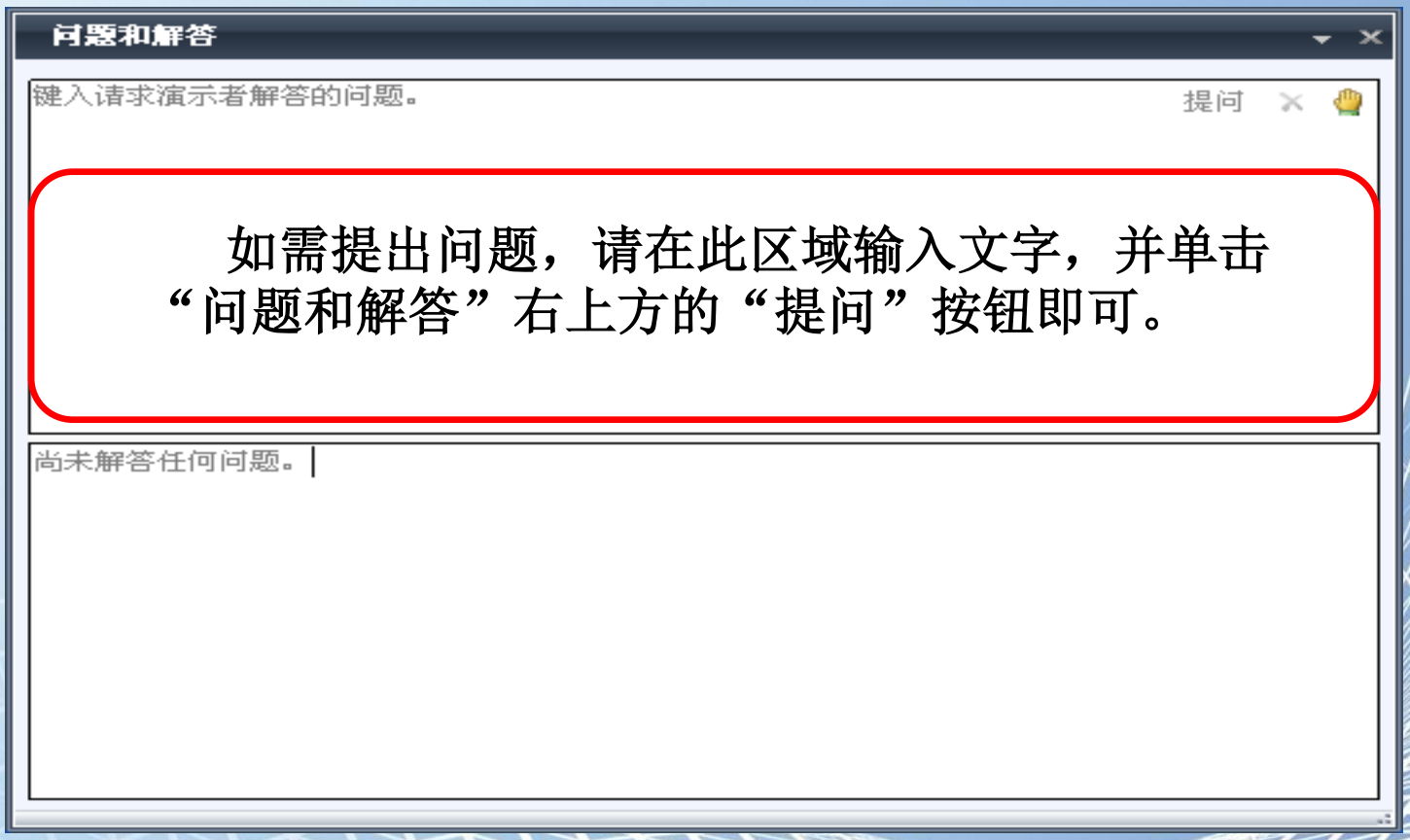
Win32k 缓冲区溢出漏洞 - CVE-2013-1333

- 如果 Windows 内核模式驱动程序不正确地处理内存中的对象，则存在一个特权提升漏洞。成功利用此漏洞的攻击者可能导致系统不稳定。

Win32k 窗口句柄漏洞 - CVE-2013-1334

- 如果 Windows 内核模式驱动程序不正确地处理内存中的对象，则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。

Question & Answer



Microsoft | TechNet


Microsoft | TechNet
Be what's next.™