微软月度信息安全公告
2013年10月

苏鹏
特约讲师

Microsoft | TechNet

议程

- 安全公告
  - MS13-080~MS13-087
- 问与答

2013年10月安全公告概述

- 新发布的安全公告
  - 严重级 MS12-080~083
  - 重要级 MS12-084~087

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 MS13-080 - 严重

公告标题	Internet Explorer 的累积性安全更新 (2879017)
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、Internet Explorer 10 和 Internet Explorer 11，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、Internet Explorer 10 和 Internet Explorer 11，此安全更新的等级为“中等”
可能的攻击方式	此安全更新可解决 Internet Explorer 中一个公开披露的漏洞和九个秘密报告的漏洞。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

Internet Explorer 中的多个内存损坏漏洞

漏洞标题	CVE 编号
Internet Explorer 内存损坏漏洞	CVE-2013-3871
Internet Explorer 内存损坏漏洞	CVE-2013-3872
Internet Explorer 内存损坏漏洞	CVE-2013-3873
Internet Explorer 内存损坏漏洞	CVE-2013-3874
Internet Explorer 内存损坏漏洞	CVE-2013-3875
Internet Explorer 内存损坏漏洞	CVE-2013-3882
Internet Explorer 内存损坏漏洞	CVE-2013-3885
Internet Explorer 内存损坏漏洞	CVE-2013-3886
Internet Explorer 内存损坏漏洞	CVE-2013-3893
Internet Explorer 内存损坏漏洞	CVE-2013-3897

Microsoft 安全公告 MS13-081 – 严重

公告标题	Windows 内核模式驱动程序中的漏洞可能允许远程执行代码 (2870008)
受影响软件	对于 Microsoft Windows（Windows 8.1、Windows Server 2012 R2 和 Windows RT 8.1 除外）的所有受支持版本，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 Microsoft Windows 中秘密报告的 7 个漏洞。如果用户查看嵌入 OpenType 或 TrueType 字体文件的共享内容，则这些漏洞中最严重的漏洞可能允许远程执行代码
受攻击的影响	远程执行代码

OpenType 字体分析漏洞 - CVE-2013-3128

- Windows 分析特制 OpenType 字体 (OTF) 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运行内核模式中的任意代码

Windows USB 描述符漏洞 - CVE-2013-3200

- 如果 Windows USB 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运行内核模式中的任意代码

Win32k 释放后使用漏洞 - CVE-2013-3879

- 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运行内核模式中的任意代码

应用容器特权提升漏洞 - CVE-2013-3880

- Windows 应用容器中存在一个特权提升漏洞。

Win32k 空页漏洞 - CVE-2013-3881

- 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运行内核模式中的任意代码。攻击者随后可安装程序；查看、更改或删除数据；或者创建拥有完全管理权限的新帐户。

DirectX 图形内核子系统双重提取漏洞 - CVE-2013-3888

- 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。成功利用此漏洞的攻击者可以运行内核模式中的任意代码。

TrueType 字体 CMAP 表漏洞 - CVE-2013-3894

- Windows 分析特制 TrueType 字体 (TTF) 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运行内核模式中的任意代码。攻击者随后可安装程序；查看、更改或删除数据；或者创建拥有完全管理权限的新帐户。

Microsoft 安全公告 MS13-082 – 严重

公告标题	.NET Framework 中的漏洞可能允许远程执行代码 (2878890)
受影响软件	对于受影响的 Microsoft Windows 版本上的 Microsoft .NET Framework 3.0 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”；对于受影响的 Microsoft Windows 版本上的 Microsoft .NET Framework 2.0 Service Pack 2 和 Microsoft .NET Framework 3.5 Service Pack 1，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 .NET Framework 中两个秘密报告的漏洞和一个公开披露的漏洞。如果用户使用能够实例化 XBAP 应用程序的浏览器访问包含特制 OpenType 字体 (OTF) 文件的网站，则最严重的漏洞可能允许远程执行代码
受攻击的影响	远程执行代码

OpenType 字体分析漏洞 - CVE-2013-3128

- 受影响的组件处理特制 OpenType 字体 (OTF) 的方式中存在一个远程执行代码漏洞。如果用户访问托管包含特制 OTF 文件的 XAML 浏览器应用程序 (XBAP) 的网站，则该漏洞可能允许远程执行代码

实体扩展漏洞 - CVE-2013-3860

- .NET Framework 中存在一个拒绝服务漏洞，该漏洞可能允许攻击者导致服务器或应用程序崩溃或无响应。

JSON 分析漏洞 - CVE-2013-3861

- .NET Framework 中存在一个拒绝服务漏洞，该漏洞可能允许攻击者导致服务器或应用程序崩溃或无响应。

Microsoft 安全公告 MS13-083 – 严重

公告标题	Windows 公共控件库中的漏洞可能允许远程执行代码 (2864058)
受影响软件	对于 Microsoft Windows 所有受支持的 64 位版本，此安全更新的等级为“严重”。对于 Windows RT 以及 Windows Server 2003、Windows Vista、Windows Server 2008、Windows 7 和 Windows 8 的所有受支持的 32 位版本，此安全更新没有严重等级
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。如果攻击者将特制的 Web 请求发送到受影响的系统上运行的 ASP .NET Web 应用程序，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

Comctl32 整数溢出漏洞 - CVE-2013-3195

- Windows 公共控件库为数据结构分配内存的方式中存在一个远程执行代码漏洞。如果攻击者将特制的 Web 请求发送到受影响的系统上运行的 ASP .NET Web 应用程序，该漏洞可能允许远程执行代码。

Microsoft 安全公告 MS13-084 – 重要

公告标题	Microsoft SharePoint Server 中的漏洞可能允许远程执行代码 (2885089)
受影响软件	对于 Microsoft SharePoint Server 2007、Microsoft SharePoint Server 2010、Microsoft SharePoint Server 2013、Microsoft SharePoint Services 3.0 和 Microsoft SharePoint Foundation 2010 的受支持版本，此安全更新的等级为“重要”。对于 Microsoft SharePoint Server 2007、Microsoft SharePoint Server 2010 和 Microsoft SharePoint Server 2013 受支持版本上受影响的 Microsoft Office Services 和 Web Apps，此安全更新的等级也为“重要”
可能的攻击方式	此安全更新可解决 Microsoft Office Server 软件中两个秘密报告的漏洞。如果用户在 Microsoft SharePoint Server、Microsoft Office Services 或 Web Apps 的受影响版本中打开特制 Office 文件，则最严重的漏洞可能允许远程执行代码
受攻击的影响	远程执行代码

Microsoft Excel 内存损坏漏洞 - CVE-2013-3889

- 受影响的 Microsoft Office 服务和 Web 应用程序分析特制文件中的内容的方式中存在一个远程执行代码漏洞。

参数注入漏洞 - CVE-2013-3895

- Microsoft SharePoint Server 中存在一个特权提升漏洞。成功利用此漏洞的攻击者可能执行跨站点脚本攻击并在登录用户的安全上下文中运行脚本。

Microsoft 安全公告 MS13-085 – 重要

公告标题	Microsoft Excel 中的漏洞可能允许远程执行代码 (2885080)
受影响软件	对于 Microsoft Office 2007、Microsoft Office 2010、Microsoft Office 2013、Microsoft Office 2013 RT 和 Microsoft Office for Mac 2011 的所有受支持版本，此安全更新的等级为“重要”。对于 Microsoft Excel Viewer 和 Microsoft Office 兼容包的受支持版本，此安全更新的等级也为“重要”
可能的攻击方式	此安全更新解决 Microsoft Office 中两个秘密报告的漏洞。如果用户使用受影响的 Microsoft Excel 版本或者其他受影响的 Microsoft Office 软件打开特制的 Office 文件，则这些漏洞可能允许远程执行代码
受攻击的影响	特权提升

Microsoft Excel 内存损坏漏洞 - CVE-2013-3889

- Microsoft Excel 分析 Excel 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。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。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。

Microsoft Excel 内存损坏漏洞 - CVE-2013-3890

- Microsoft Excel 分析 Excel 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 MS13-086 – 重要

公告标题	Microsoft Word 中的漏洞可能允许远程执行代码 (2885084)
受影响软件	对于 Microsoft Word 2003、Microsoft Word 2007 和 Microsoft Office 兼容包的受支持版本，此安全更新的等级为“重要”
可能的攻击方式	此安全更新解决 Microsoft Office 中两个秘密报告的漏洞 。如果特制文件在 Microsoft Word 的受影响版本或其他受影响的 Microsoft Office 软件中打开，则这些漏洞可能允许远程执行代码
受攻击的影响	远程执行代码

内存损坏漏洞 - CVE-2013-3891

- 受影响的 Microsoft Word 软件分析特制文件的方式中存在远程执行代码漏洞。成功利用此漏洞的攻击者可以完全控制受影响的系统

内存损坏漏洞 - CVE-2013-3892

- 受影响的 Microsoft Word 软件分析特制文件的方式中存在远程执行代码漏洞。

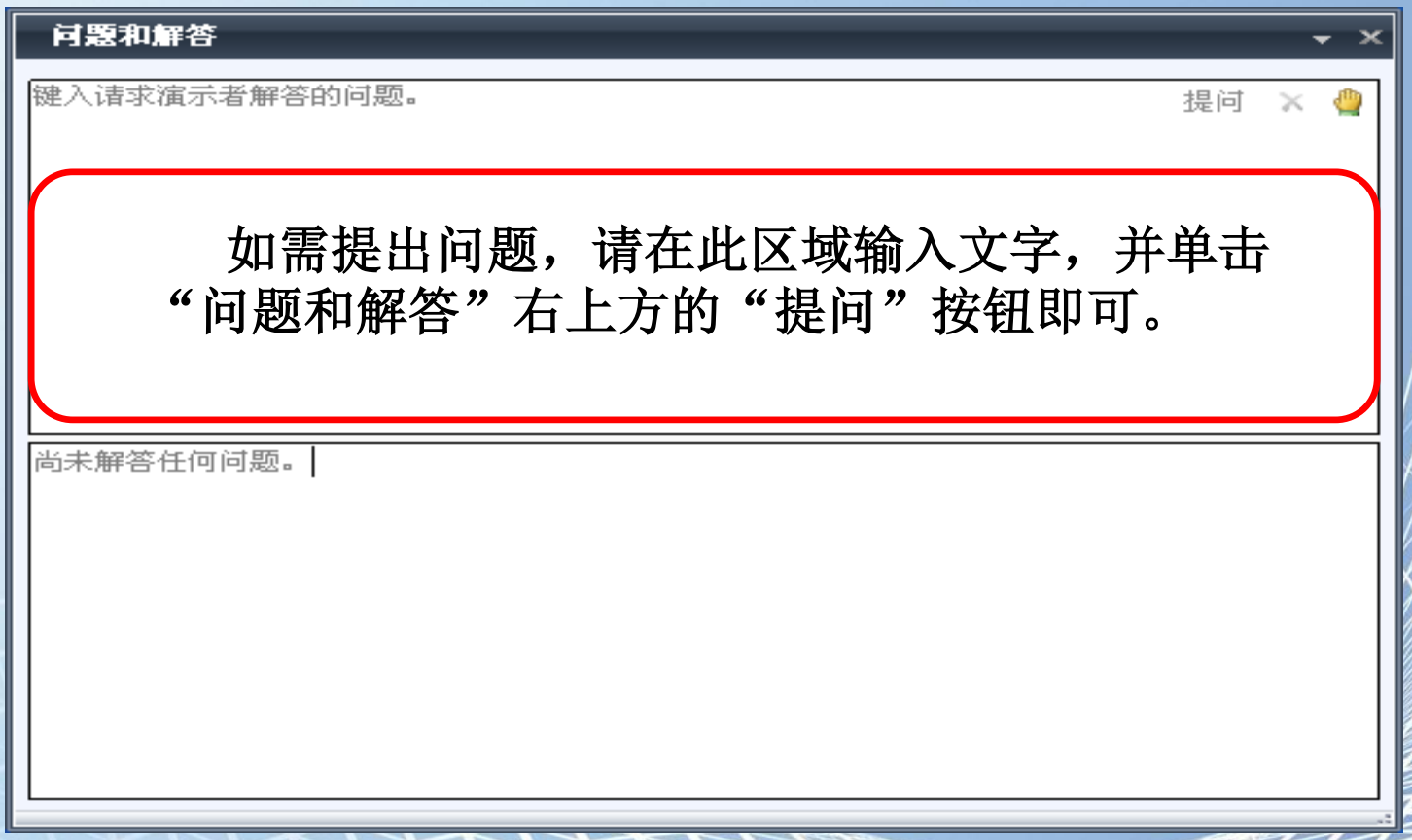
Microsoft 安全公告 MS13-087 – 重要

公告标题	Silverlight 中的漏洞可能允许信息泄露 (2890788)
受影响软件	对于安装在 Mac 和所有受支持的 Microsoft Windows 版本上的 Microsoft Silverlight 5 和 Microsoft Silverlight 5 Developer Runtime，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 Silverlight 中一个秘密报告的漏洞。如果攻击者拥有包含旨在利用此漏洞的特制 Silverlight 应用程序的网站，然后诱使用户查看该网站，则该漏洞可能允许信息泄露
受攻击的影响	信息泄露

Silverlight 漏洞 - CVE-2013-3896

- Silverlight 处理内存中的特定对象的方式中存在一个信息泄露漏洞。

Question & Answer



Microsoft | TechNet


Microsoft | TechNet
Be what's next.™