微软月度信息安全公告
2013年12月

苏鹏
特约讲师

Microsoft | TechNet

议程

- 安全公告
  - MS13-088~MS13-095
- 问与答

2013年12月安全公告概述

- 新发布的安全公告
  - 严重级 MS13-096,097,098,099,105
  - 重要级 MS13-100,101,102,103,104,106

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 MS13-096 - 严重

公告标题	Microsoft Graphics 组件中的漏洞可能允许远程执行代码 (2908005)
受影响软件	对于 Windows Vista、Windows Server 2008、Microsoft Office2003、Microsoft Office2007、Microsoft Office 2010 和 Microsoft Office 兼容包的所有受支持版本，此安全更新的等级为“严重”。对于Microsoft Lync 2010 和 Microsoft Lync 2013 的所有受支持版本，它的等级为“重要”。
可能的攻击方式	此安全更新可解决 Microsoft Windows、Microsoft Office 和 Microsoft Lync 中一个公开披露的漏洞 如果用户查看包含特制 TIFF 文件的内容，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

Microsoft 图形组件内存损坏漏洞 - CVE-2013-3906

- 受影响的 Windows 组件和其他受影响的软件处理特制 TIFF 文件的方式中存在一个远程执行代码漏洞。如果用户查看共享内容中的 TIFF 文件，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完全控制受影响的系统。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 MS13-097 – 严重

公告标题	Internet Explorer 的累积性安全更新 (2898785)
受影响软件	对于受影响的 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”；对于受影响的 Windows 服务器上的 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“重要”；对于受支持的 Windows Server 2003 版本上的 Internet Explorer 6，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 7 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 中的多个特权提升漏洞

- 验证本地文件安装期间和安全创建注册表项期间，Internet Explorer 中存在特权提升漏洞

漏洞标题	CVE 编号
Internet Explorer 特权提升漏洞	CVE-2013-5045
Internet Explorer 特权提升漏洞	CVE-2013-5046

Internet Explorer 中的多个内存损坏漏洞

- 当 Internet Explorer 不正确地访问内存中的对象时，存在远程执行代码漏洞。这些漏洞可能以一种攻击者可以在当前用户的上下文中执行任意代码的方式损坏内存

漏洞标题	CVE 编号
Internet Explorer 内存损坏漏洞	CVE-2013-5047
Internet Explorer 内存损坏漏洞	CVE-2013-5048
Internet Explorer 内存损坏漏洞	CVE-2013-5049
Internet Explorer 内存损坏漏洞	CVE-2013-5051
Internet Explorer 内存损坏漏洞	CVE-2013-5052

Microsoft 安全公告 MS13-098 – 严重

公告标题	Windows 中的漏洞可能允许远程执行代码 (2893294)
受影响软件	对于 Windows 所有受支持的版本，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 中一个秘密报告的漏洞。如果用户或应用程序在受影响的系统上运行或安装特制的、经过签名的可移植可执行 （PE) 文件，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

WinVerifyTrust 签名验证漏洞 - CVE-2013-3900

- WinVerifyTrust 函数处理可移植可执行文件 (PE) 的 Windows Authenticode 签名验证的方式中存在一个远程执行代码漏洞。匿名攻击者可以通过修改经过签名的现有可执行文件以利用文件的未验证部分来利用此漏洞，从而向文件添加恶意代码，而无需使签名无效。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 MS13-099 – 严重

公告标题	Microsoft 脚本运行时对象库中的漏洞可能允许远程执行代码 (2909158)
受影响软件	对于所有支持的 Microsoft Windows 版本上受影响的 Windows Script 5.6、Windows Script 5.7 和 Windows Script 5.8，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 中一个秘密报告的漏洞。如果攻击者诱使用户访问特制网站或者托管特制内容的网站，则此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 脚本运行时对象库中的释放后使用漏洞 - CVE-2013-5056

- 这是 Microsoft 脚本运行时对象库中的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 MS13-105 – 严重

公告标题	Microsoft Exchange Server 中的漏洞可能允许远程执行代码 (2915705)
受影响软件	Microsoft Exchange Server 2007、Microsoft Exchange Server 2010 和 Microsoft Exchange Server 2013 的所有受支持版本，此安全更新等级为“严重”。
可能的攻击方式	此安全更新解决 Microsoft Exchange Server 中三个公开披露的漏洞和一个秘密报告的漏洞。Microsoft Exchange Server 的 WebReady Document Viewing 和数据丢失防护功能中存在最严重的漏洞。如果攻击者向受影响的 Exchange Server 中的用户发送包含特制文件的电子邮件，则这些漏洞可能允许在 LocalService 帐户的安全上下文中远程执行代码。LocalService 帐户在本地系统上具有最低特权，在网络上提供匿名凭据。
受攻击的影响	远程执行代码

Oracle Outside In 包含多个可利用的漏洞

- 如果用户在浏览器中通过 Outlook Web Access 查看特制文件，则这些漏洞可能允许作为 LocalService 帐户远程执行代码。成功利用此漏洞的攻击者可能在受影响的 Exchange Server 上作为本地服务帐户运行代码。LocalService 帐户在本地计算机上具有最低特权，在网络上提供匿名凭据。

Mac 已禁用漏洞 - CVE-2013-1330

- Microsoft Exchange Server 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在 Outlook Web Access (OWA) 服务帐户的上下文中运行任意代码。

OWA XSS 漏洞 – CVE-2013-5072

- Microsoft Exchange Server 中存在一个特权提升漏洞。成功利用此漏洞的攻击者可以在当前用户的上下文中运行脚本。

Microsoft 安全公告 MS13-100 – 重要

公告标题	Microsoft SharePoint Server 中的漏洞可能允许远程执行代码 (2904244)
受影响软件	对于 Microsoft SharePoint Server 2013 的受支持版本，Microsoft SharePoint Server 2010 和 Microsoft SharePoint Server 2013 的受支持版本上的受影响的 Microsoft Office Services 和 Web Apps，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 服务器软件中多个秘密报告的漏洞。如果经过身份验证的攻击者向 SharePoint 服务器发送特制网页内容，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

SharePoint 网页内容漏洞 - CVE-2013-5059

- Microsoft SharePoint Server 中存在远程执行代码漏洞。成功利用这些漏洞的经过身份验证的攻击者可以在 W3WP 服务帐户的安全上下文中运行任意代码。

Microsoft 安全公告 MS13-101 – 重要

公告标题	Windows 内核模式驱动程序中的漏洞可能允许特权提升 (2880430)
受影响软件	对于 Windows XP、Windows Server 2003、Windows Vista、Windows Server 2008 、Windows7、Windows Server 2008 R2、Windows 8、Windows Server 2012 和 Windows RT 的所有受支持的版本，此安全更新的等级为“重要”。对于 Windows 8.1、Windows Server 2012 和 Windows RT 8.1，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 Microsoft Windows 中秘密报告的五个漏洞。如果攻击者登录某个系统并运行特制应用程序，更严重的漏洞可能允许特权提升
受攻击的影响	特权提升、拒绝服务

Win32k 整数溢出漏洞 - CVE-2013-3899

- Win32k.sys 内核模式驱动程序验证内存中的地址值的方式中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。

Win32k 释放后使用漏洞 - CVE-2013-3902

- Microsoft Windows 内核模式驱动程序中存在一个特权提升漏洞。当 Windows 内核不正确地处理内存中的对象时，会导致该漏洞

TrueType 字体分析漏洞 - CVE-2013-3903

- Microsoft Windows 内核中存在一个拒绝服务漏洞。当 Windows 内核不正确地处理特制的 TrueType 字体文件时，会导致此漏洞。

端口级驱动程序双重提取漏洞 - CVE-2013-3907

- Windows 音频端口级驱动程序 (portcls.sys) 处理内存中的对象的方式中存在一个特权提升漏洞。

Win32k 整数溢出漏洞 - CVE-2013-5058

- Win32k.sys 内核模式驱动程序处理内存中的对象的方式中存在一个拒绝服务漏洞。成功利用此漏洞的攻击者可能会导致目标系统停止响应。

Microsoft 安全公告 MS13-102 – 重要

公告标题	LRPC 客户端中的漏洞可能允许特权提升 (2898715)
受影响软件	对于 Windows XP 和 Windows Server 2003 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。如果攻击者欺骗 LRPC 服务器并向任何 LRPC 客户端发送特制 LPC 端口消息，则该漏洞可能允许特权提升
受攻击的影响	特权提升

LRPC 客户端缓冲区溢出漏洞 - CVE-2013-3878

- Microsoft 本地远程过程调用 (LRPC) 中存在一个特权提升漏洞，攻击者哄骗 LRPC 服务器并使用特制 LPC 端口消息在 LRPC 客户端上导致基于堆栈的缓冲区溢出情形。LRPC 在内部使用 Microsoft 本地过程调用 (LPC)。因此，实际上，如果未正确实施，任何 LPC 消费者都可能受此漏洞影响

Microsoft 安全公告 MS13-103 – 重要

公告标题	ASP.NET SignalR 中的漏洞可能允许特权提升 (2905244)
受影响软件	对于 ASP.NET SignalR 版本 1.1.0、1.1.1、1.1.2、1.1.3 和 2.0.0 以及 Microsoft Visual Studio Team Foundation Server 2013 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	此安全更新可解决 ASP.NET SignalR 中一个秘密报告的漏洞。如果攻击者将特制 JavaScript 反映回目标用户的浏览器，则该漏洞可能允许特权提升
受攻击的影响	特权提升

SignalR XSS 漏洞 – CVE-2013-5042

- ASP.NET SignalR 中存在一个特权提升漏洞，可能允许攻击者在目标用户的上下文中访问资源。

Microsoft 安全公告 MS13-104 – 重要

公告标题	Microsoft Office 中的漏洞可能允许信息泄露 (2909976)
受影响软件	对于 Microsoft Office 2013 和 Microsoft Office 2013 RT 软件的受支持版本，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 中一个秘密报告的漏洞，如果用户尝试打开恶意网站上托管的 Office 文件，则该漏洞可能允许信息泄露
受攻击的影响	信息泄露

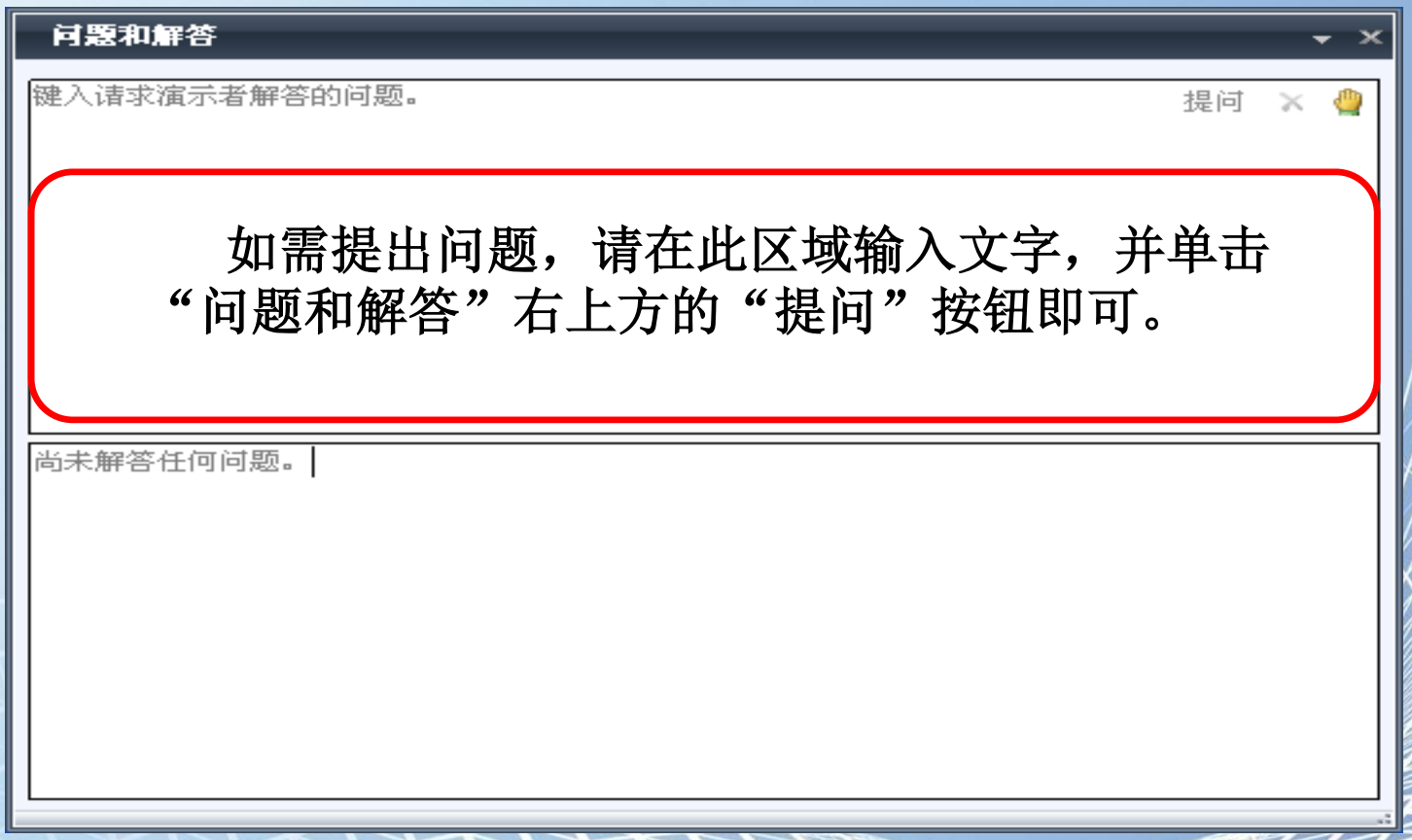
令牌劫持漏洞 - CVE-2013-5054

- 如果受影响的 Microsoft Office 软件尝试打开恶意网站上托管的 Office 文件时未正确处理特制响应，则存在一个信息泄露漏洞。

Microsoft 安全公告 MS13-106 – 重要

公告标题	Microsoft Office 中的漏洞可能允许信息泄露 (2909976)
受影响软件	对于 Microsoft Office 2007和 Microsoft Office 2010 软件的受支持版本，此安全更新的等级为“重要”
可能的攻击方式	此安全更新解决了 Microsoft Office 共享组件中 目前正在被利用的一个公开披露的漏洞。如果用户在能够实例化 COM 组件（如 Internet Explorer）的 Web 浏览器中查看特制网页，则该漏洞可能允许安全功能绕过
受攻击的影响	安全功能绕过

Question & Answer



Microsoft | TechNet


Microsoft | TechNet
Be what's next.™