微软月度信息安全公告
2013年11月

苏鹏
特约讲师

Microsoft | TechNet

议程

- 安全公告
  - MS13-088~MS13-095
- 问与答

2013年11月安全公告概述

- 新发布的安全公告
  - 严重级 MS12-088~090
  - 重要级 MS12-091~095

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 MS13-088 - 严重

公告标题	Internet Explorer 的累积性安全更新 (2888505)
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 6、Internet Explorer 7、Internet Explorer 8、Internet Explorer 9、Internet Explorer 10 和 Internet Explorer 10，此安全更新的等级为“中等”。此外，对于受影响的 Windows 服务器上的 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 中的 10 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 信息泄露漏洞 - CVE-2013-3908

- Internet Explorer 在生成打印预览时处理特制 Web 内容的方式中存在一个信息泄露漏洞。

Internet Explorer 信息泄露漏洞 - CVE-2013-3909

- Internet Explorer 处理 CSS 特殊字符的方式中存在一个信息泄露漏洞。如果用户查看网页，攻击者可通过构建一个允许信息泄露的特制网页来利用此漏洞。成功利用此漏洞的攻击者可查看其他域或 Internet Explorer 区域中的内容。

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-2013-3910
Internet Explorer 内存损坏漏洞	CVE-2013-3911
Internet Explorer 内存损坏漏洞	CVE-2013-3912
Internet Explorer 内存损坏漏洞	CVE-2013-3914
Internet Explorer 内存损坏漏洞	CVE-2013-3915
Internet Explorer 内存损坏漏洞	CVE-2013-3916
Internet Explorer 内存损坏漏洞	CVE-2013-3917

Microsoft 安全公告 MS13-089 – 严重

公告标题	Windows 图形设备接口中的漏洞可能允许远程执行代码 (2876331)
受影响软件	对于 Microsoft 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。如果用户在写字板中查看或打开特制 Windows Write 文件，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

图形设备接口整数溢出漏洞 - CVE-2013-3940

- Windows 图形设备接口 (GDI) 在写字板中处理特制 Windows Write 文件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 安全公告 MS13-090 – 严重

公告标题	ActiveX Kill Bit 的累积性安全更新 (2900986)
受影响软件	对于 Windows XP、Windows Vista、Windows 7、Windows 8、Windows RT、Windows 8.1 和 Windows RT 8.1 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、Windows Server 2008 R2、Windows Server 2012 和 Windows Server 2012 R2 的所有受支持版本，此安全更新的等级为“中等”
可能的攻击方式	此安全更新解决了当前正被利用的一个秘密报告的漏洞。InformationCardSigninHelper 类 ActiveX 控件中存在该漏洞。如果用户使用实例化 ActiveX 控件的 Internet Explorer 查看特制网页，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

InformationCardSigninHelper 漏洞 - CVE-2013-3918

- InformationCardSigninHelper 类 ActiveX 控件 icardie.dll 中存在一个远程执行代码漏洞。攻击者可以通过构造特制网页来利用该漏洞。当用户查看网页时，该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当前用户相同的用户权限

Microsoft 安全公告 MS13-091 – 严重

公告标题	Microsoft Office 中的漏洞可能允许远程执行代码 (2885093)
受影响软件	对于 Microsoft Office 2003、Microsoft Office 2007、Microsoft Office 2010、Microsoft Office 2013 和 Microsoft Office 2013 RT 软件的所有受支持版本，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 Microsoft Office 中 3 个秘密报告的漏洞。如果受影响的在 Microsoft Office 软件版本中打开特制 WordPerfect 文档文件，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

WPD 文件格式内存损坏漏洞 - CVE-2013-0082

- 受影响的 Microsoft Office 软件分析特制 WordPerfect 文档 (.wpd) 文件的方式中存在一个远程执行代码漏洞

Word 堆栈缓冲区覆盖漏洞 - CVE-2013-1324

- 受影响的 Microsoft Office 软件分析特制 WordPerfect 文档文件的方式中存在一个远程执行代码漏洞

Word 堆覆盖漏洞 - CVE-2013-1325

- 受影响的 Microsoft Office 软件分析特制 WordPerfect 文档文件的方式中存在一个远程执行代码漏洞。

Microsoft 安全公告 MS13-092 – 重要

公告标题	Hyper-V 中的漏洞可能允许特权提升 (2893986)
受影响软件	对于 Windows 8（用于基于 x64 的系统）和 Windows Server 2012，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 Windows 中一个秘密报告的漏洞。如果攻击者将虚拟化调用中的特制函数参数从当前运行的虚拟机传递到虚拟机监控程序，则该漏洞可能允许特权提升
受攻击的影响	特权提升

地址损坏漏洞 - CVE-2013-3898

- Windows 8 和 Windows Server 2012 上的 Hyper-V 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共享的 Hyper-V 主机上的另一虚拟机 (VM) 中以系统身份执行任意代码。攻击者不能在 Hyper-V 主机上执行代码，而只能在同一主机上的来宾虚拟机上执行。该漏洞也可能在相同平台上的 Hyper-V 中允许拒绝服务，这允许攻击者导致 Hyper-V 主机停止响应或重新启动。

Microsoft 安全公告 MS13-093 – 重要

公告标题	Windows 辅助功能驱动程序中的漏洞可能允许信息泄露 (2875783)
受影响软件	对于 Windows XP、Windows Server 2003、Windows Vista、Windows Server 2008、Windows 7、Windows Server 2008 R2、Windows 8 和 Windows Server 2012 所有受支持的 64 位版本，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 Windows 中一个秘密报告的漏洞。如果攻击者以本地用户身份登录受影响的系统，并且在系统上运行旨在使攻击者从特权较高的帐户中获取信息的应用程序，则此漏洞可能允许信息泄露
受攻击的影响	信息泄露

辅助功能驱动程序信息泄露漏洞 - CVE-2013-3887

- 当 Windows 内核模式驱动程序不正确地处理内核和用户内存之间的数据复制时，存在一个信息泄露漏洞。

Microsoft 安全公告 MS13-094 – 重要

公告标题	Microsoft Outlook 中的漏洞可能允许信息泄露 (2894514)
受影响软件	对于 Microsoft Outlook 2007、Microsoft Outlook 2010、Microsoft Outlook 2013 和 Microsoft Outlook 2013 RT 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 Microsoft Outlook 中一个公开披露的漏洞。如果用户使用受影响的 Microsoft Outlook 版本打开或预览特制的电子邮件，则此漏洞可能允许信息泄露
受攻击的影响	信息泄露

S/MIME AIA 漏洞 – CVE-2013-3905

- 当 Microsoft Outlook 无法正确处理 S/MIME 证书元数据的扩展时，存在一个信息泄露漏洞。成功利用此漏洞的攻击者可能会从目标系统和与目标系统共享网络的其他系统确定系统信息（例如，IP 地址和开放的 TCP 端口）。

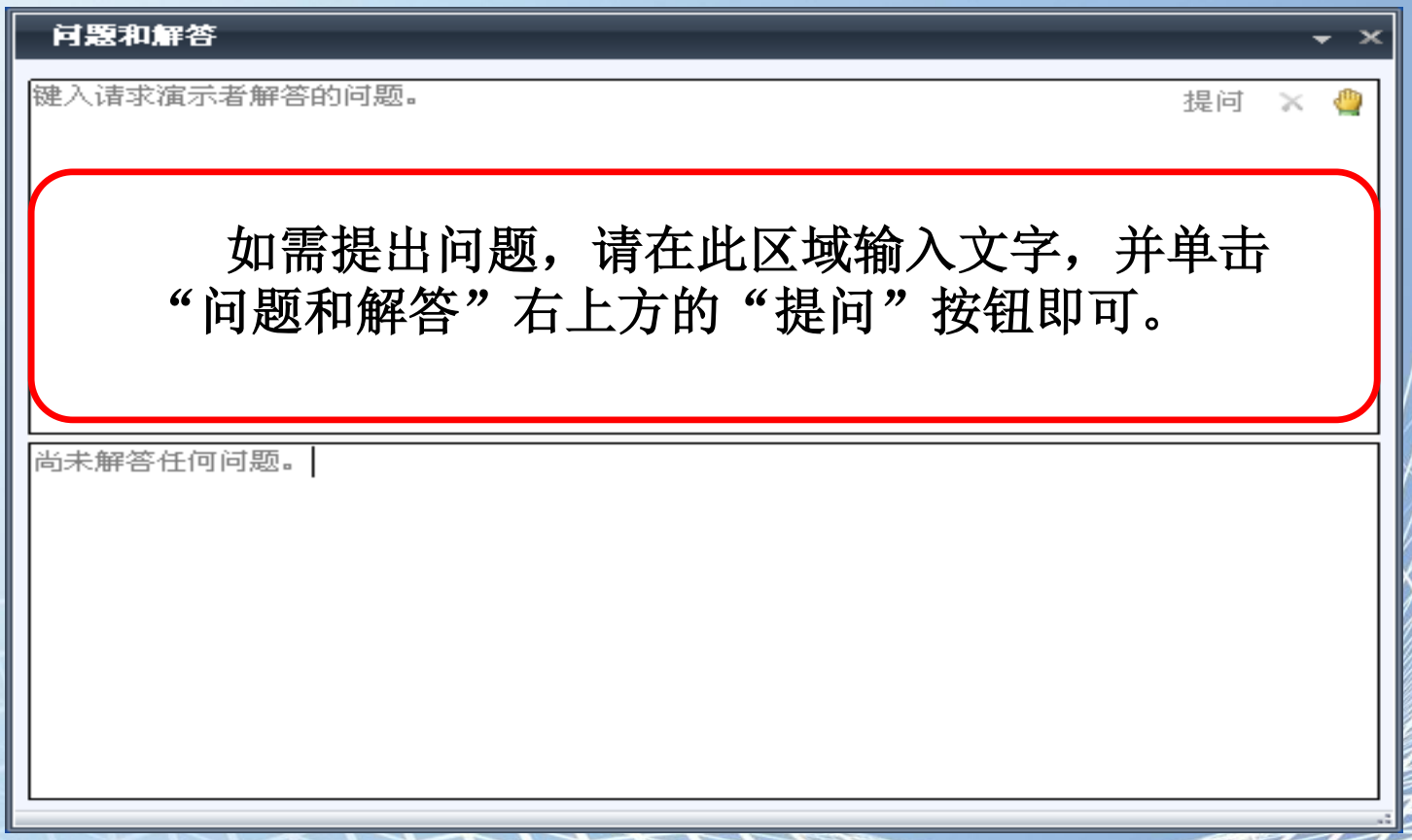
Microsoft 安全公告 MS13-095 – 重要

公告标题	数字签名中的漏洞可能允许拒绝服务 (2868626)
受影响软件	对于 Microsoft Windows 所有受支持的版本，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。当受影响的 Web 服务处理特制 X.509 证书时，此漏洞可能允许拒绝服务
受攻击的影响	拒绝服务

数字签名漏洞 - CVE-2013-3869

- X.509 证书分析的实施中存在一个拒绝服务漏洞，该漏洞可能导致受影响的 Web 服务停止响应。当 X.509 证书验证操作无法处理特制 X.509 证书时，会导致该漏洞

Question & Answer



Microsoft | TechNet


Microsoft | TechNet
Be what's next.™