微软月度信息安全公告
2013年4月

苏鹏
特约讲师

Microsoft | TechNet

议程

- 安全公告
  - MS13-028~MS13-036
- 问与答

2013年4月安全公告概述

- 新发布的安全公告
  - 严重级 MS12-028,029
  - 重要级 MS12-030,031,032,033,034,035,036

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 MS13-028 - 严重

公告标题	Internet Explorer 的累积性安全更新 (2817183)
受影响软件	Internet Explorer 6、Internet Explorer 7、Internet Explorer 8、Internet Explorer 9 和 Internet Explorer 10，
可能的攻击方式	此安全更新可解决 Internet Explorer 中两个秘密报告的漏洞。如果用户使用 Internet Explorer 查看特制网页，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

Internet Explorer 中的多个释放后使用漏洞

漏洞标题	CVE 编号
Internet Explorer 释放后使用漏洞	CVE-2013-1303
Internet Explorer 释放后使用漏洞	CVE-2013-1304

Microsoft | TechNet

Microsoft 安全公告 MS13-029 – 严重

公告标题	远程桌面客户端中的漏洞可能允许远程执行代码 (2828223)
受影响软件	对于 Windows XP、Windows Vista 和 Windows 7 上受影响的 Remote Desktop Connection 6.1 客户端和 Remote Desktop Connection 7.0 客户端，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 Windows 远程桌面客户端中一个秘密报告的漏洞。如果用户查看特制网页，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

RDP ActiveX 控件远程执行代码漏洞 - CVE-2013-1296

- 当远程桌面 ActiveX 控件 mstscax.dll 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。攻击者可通过诱使用户访问特制网页来利用该漏洞。成功利用此漏洞的攻击者可以获得与登录用户相同的用户权限。

Microsoft 安全公告 MS13-030 – 重要

公告标题	SharePoint 中的漏洞可能允许信息泄露 (2827663)
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 MS13-031 – 重要

公告标题	Windows 内核中的漏洞可能允许特权提升 (2813170)
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“重要”
可能的攻击方式	此安全更新可解决 Microsoft Windows 中两个秘密报告的漏洞。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

内核争用条件漏洞 - CVE-2013-1284

- 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。

Microsoft 安全公告 MS13-032 – 重要

公告标题	Active Directory 中的漏洞可能导致拒绝服务 (2830914)
受影响软件	对于 Microsoft Windows 服务器上的 Active Directory、Active Directory 应用程序模式 (ADAM)、Active Directory 轻型目录访问协议 (AD LDS) 和 Active Directory 服务，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 Active Directory 中一个秘密报告的漏洞。如果攻击者向轻型目录访问协议 (LDAP) 服务发送特制查询，则此漏洞可能允许拒绝服务。
受攻击的影响	拒绝服务

内存消耗漏洞 - CVE-2013-1282

- Active Directory 实施中存在一个拒绝服务漏洞，该漏洞可能导致服务停止响应。当 LDAP 服务无法处理特制查询时，会导致该漏洞。

Microsoft 安全公告 MS13-033 – 重要

公告标题	Windows 客户端/服务器运行时子系统 (CSRSS) 中的漏洞可能允许特权提升 (2820917)
受影响软件	对于 Windows XP Professional x64 Edition 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	在 Windows XP、Windows Vista、Windows Server 2003 和 Windows Server 2008 的所有受支持版本中，此安全更新可解决一个秘密报告的漏洞。如果攻击者登录系统并运行特制应用程序，则该漏洞可能允许特权提升
受攻击的影响	特权提升

CSRSS 内存损坏漏洞 - CVE-2013-1295

- 如果 Windows CSRSS 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在本地系统的上下文中运行任意代码

Microsoft 安全公告 MS13-034 – 重要

公告标题	Microsoft 反恶意软件客户端中的漏洞可能允许特权提升 (2823482)
受影响软件	对于用于 Windows 8 和 Windows RT 的 Windows Defender 受支持版本中的 Microsoft 反恶意软件客户端，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 反恶意软件客户端中一个秘密报告的漏洞。由于 Microsoft 反恶意软件客户端使用的路径名称，此漏洞可能允许特权提升
受攻击的影响	特权提升

Microsoft 反恶意软件不正确路径名称漏洞 - CVE-2013-0078

- 这是一个特权提升漏洞。成功利用此漏洞的攻击者可以在 LocalSystem 帐户的安全上下文中执行任意代码并完全控制系统。

Microsoft 安全公告 MS13-035 – 重要

公告标题	HTML 清理组件中的漏洞可能允许特权提升 (2821818)
受影响软件	对于 Microsoft SharePoint Server 2010、Microsoft Groove Server 2010、Microsoft SharePoint Foundation 2010 和 Microsoft Office Web Apps 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	此安全更新解决了 Microsoft Office 中一个秘密报告的漏洞。如果攻击者将特制内容发送给用户，则该漏洞可能允许特权提升
受攻击的影响	特权提升

HTML 清理漏洞 - CVE-2013-1289

- 清理 HTML 字符串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能在受影响的系统上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 MS13-036 – 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 (2829996)
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“重要”。
可能的攻击方式	此安全更新可解决 Microsoft Windows 中的三个秘密报告的漏洞和一个公开披露的漏洞。如果攻击者登录系统并运行特制应用程序，最严重的漏洞可能允许特权提升
受攻击的影响	特权提升

Win32k 争用条件漏洞 - CVE-2013-1283

- 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

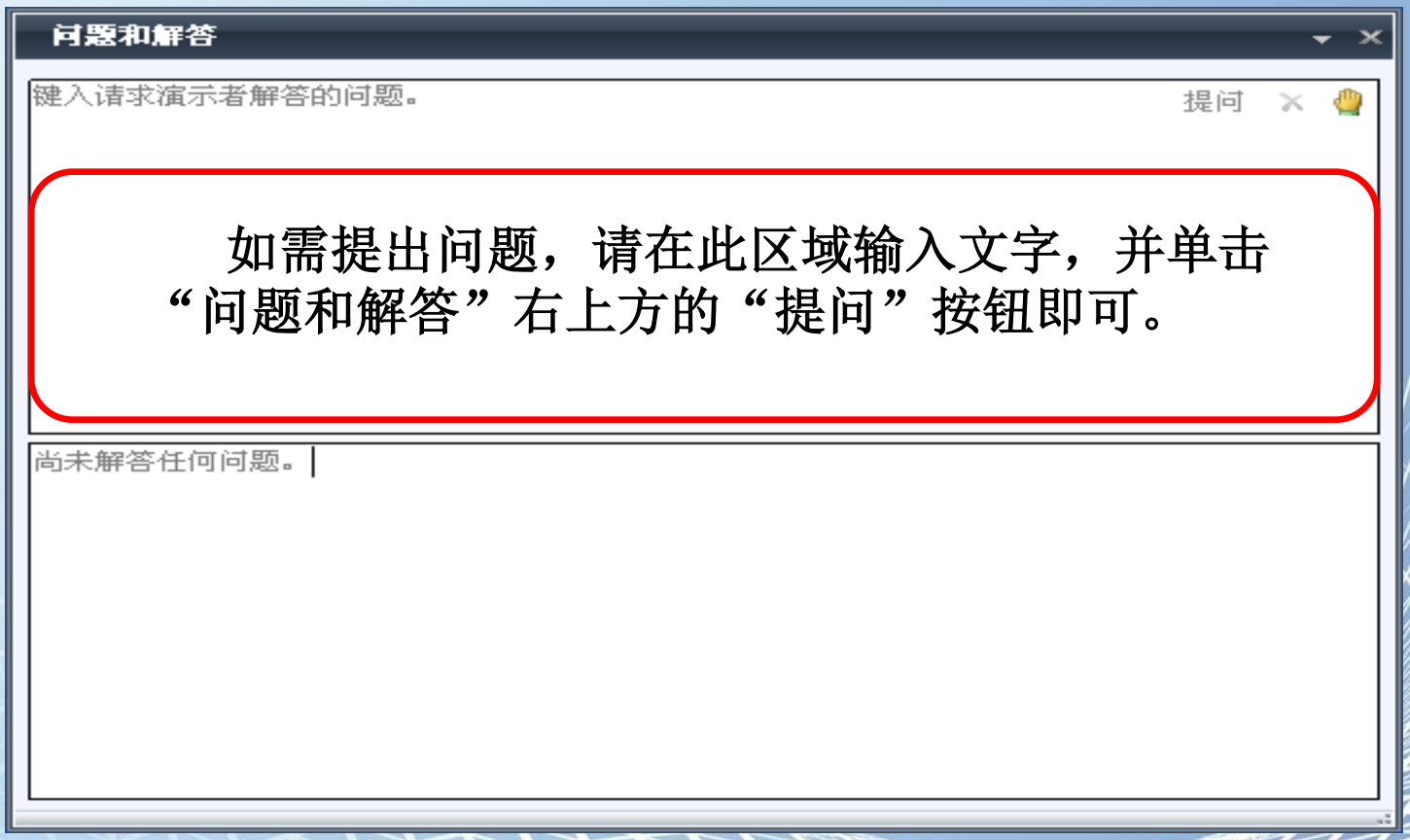
Win32k 字体分析漏洞 - CVE-2013-1291

- 当 Windows 未能处理特制字体文件时，存在一个拒绝服务漏洞。此漏洞可能会导致计算机停止响应和重新启动。

NTFS 空指针解除引用漏洞 - CVE-2013-1293

- 如果 NTFS 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。

Question & Answer



Microsoft | TechNet


Microsoft | TechNet
Be what's next.™