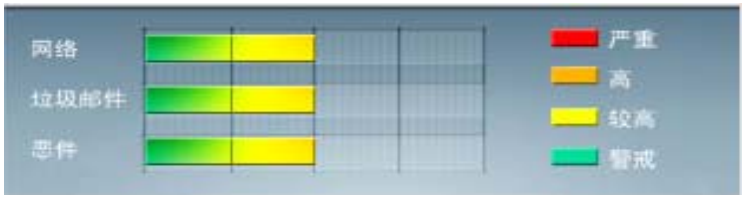
# 安全威胁每周警讯

2010/12/12～2010/12/18

本周威胁指数




***TrendMicro 中国区网络安全监控中心***

# 前十大病毒警讯

| 排名 | 病毒名称 | 威胁类型 | 风险等级 | 趋势 | 病毒行为描述 |
|---|---|---|---|---|---|
| 1 | WORM_DOWNAD.AD | 蠕虫 | ★★★★ | ↑ | 该病毒会攻击未安装微软 IE 漏洞 MS08-067 的电脑，并且会在受感染电脑产生五万个恶意程序网址并试图在同一时间内随机连结其中 500 个恶意网站下载病毒 |
| 2 | TROJ_DOWNAD.INF | 木马 | ★★★ | ↓ | Downad 蠕虫关联木马 |
| 3 | TROJ_IFRAME.CP | 木马 | ★★★ | ↓ | GIF、jpg 和 SWF 文件中被插入一个恶意的 iframe 标记时，趋势科技会将其判断为 TROJ_IFRAME.CP 病毒。当这些文件被执行时，会重定向到这些 URL，并下载恶意程序 |
| 4 | WORM_DOWNAD | 蠕虫 | ★★★★ | ↓ | 该病毒会攻击未安装微软 IE 漏洞 MS08-067 的电脑，并且会在受感染电脑产生五万个恶意程序网址并试图在同一时间内随机连结其中 500 个恶意网站下载病毒 |
| 5 | Cryp_Xed-12 | 木马 | ★★★ | → | 疑似病毒 |
| 6 | CRCK_KEYGEN | 破解程序 | ★★ | ↑ | 非法破解程序 |
| 7 | WORM_ECODE.E-CN | 蠕虫 | ★★★★ | ↓ | E 语言编写的蠕虫病毒，会通过 U 盘进行传播，特征是在文件夹下建立同名 exe 文件 |
| 8 | PAK_Generic.001 | 加壳文件 | ★★ | ↑ | 对加壳文件的通用检测。病毒通常会使用加壳手法来达到不被杀毒软件检测的目的 |
| 9 | GRAY_Gen | 间谍软件 | ★★ | ↑ | 间谍软件的通用检测名。在用户不知情的情况下，在其电脑上安装后门、收集用户信息的软件。 |
| 10 | HTML_IFRAME.AZ | 网页病毒 | ★★ | ↓ | 网页病毒，通常在网页在插入一个恶意 iframe，用户在访问该网页时会下载恶意文件或重定向到恶意网站 |

# 系统漏洞信息

**MS10-091:OpenType 字体 (OTF) 驱动程序中的漏洞可能允许远程执行代码 (2296199)**

**受影响的软件:**

Window xp

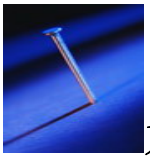
Windows Server 2003

Windows Vista

Windows Server 2008

Windows 7

**描述:** 请见http://www.microsoft.com/china/technet/security/bulletin/MS10-091.mspx



# 系统安全技巧

摘要: Internet 网络中既有明媚阳光，也有潜流暗壑，在该网络中尽情冲浪时，稍微不留神可能会遭遇到各式各样的“骚扰”，会拖累上网访问的效率，更有可能引来安全威胁。那么我们就来采取一些安全应对措施，让上网冲浪少受安全“骚扰”。

Internet 网络中既有明媚阳光,也有潜流暗壑,在该网络中尽情冲浪时,稍微不留神可能会遭 遇到各式各样的“骚扰”,会拖累上网访问的效率，更有可能引来安全威胁。既然知道上网冲浪有可能会遭遇这么多“骚扰”，那么我们为什么在冲浪之前不采取安 全应对措施，来让上网冲浪少受安全“骚扰”呢?

禁止使用点对点工作模式

一般来说，无线局域网中的普通工作站常常有两种基本的工作传输模式，一种模式就是基础架构模式， 另外一种就是点对点工作模式。当无线局域网网络采用基础架构模式工作时，那么局域网中的所有无线工作站都需要通过一个无线路由器设备来进行信号处理；换句 话说，无论我们是上网浏览网页内容，还是与相同局域网中的其他工作站进行共享传输交流，无线工作站的所有数据信号都需要经过无线路由器设备。大多数单位的 无线局域网网络都属于这种类型的网络。

如果无线局域网网络采用点对点模式工作时，那么无线局域网中工作站与工作站之间的相互通信能够直 接进行，而不需借助一个无线路由器设备或其他无线节点设备。在一些特定的场合下，这种工作模式比较有利于工作站的快速网络访问，比方说要是我们想与局域网 中其他工作站进行共享传输文件时，就可以选用点对点工作模式。不过比较麻烦的是，只要我们启用了点对点这种模式，那么本地无线网络附近的非法用户也能够在 我们毫无知情的情况下偷偷访问本地网络中的重要隐私信息，这么一来本地无线局域网的工作安全性就会大大下降。

为了有效避免本地网络中的隐私信息对外泄露，我们强烈建议大家取消使用点对点工作模式，除非在万不得已的情况下，再启用该工作模式，而且一旦完成工作站之间的信息交流任务之后，必须立即再禁用点对点工作模式。

拒绝广播无线网络标识符

为了方便无线局域网中的普通工作站能够快速地发现连接无线节点设备,每一个无线节点设备基本都有 一个网络服务标识名称，这个名称信息一般被叫做无线节点的 SSID 标识符，普通工作站只有通过该标识符才能与无线节点设备建立正常的无线网络连接，要是不知道 SSID 标识符，那么普通工作站是无法加入到无线局域 网中的。因此，要想阻止非法用户偷偷使用本地的无线网络,我们必须想办法不让非法用户知道本地无线局域网的 SSID 标识符信息。

目前，市场上推出的许多无线节点设备出厂默认设置都是允许无线网络标识符广播的，一旦启用了该功 能后，就相当于无线节点设备会自动向无线覆盖范围内的所有普通工作站发布本地的无线网络标识符名称信息。尽管启用 SSID 标识符广播功能让大家能够非常方 便地加入到本地无线网络中,但是该功能同样也让一些非法用户可以轻松地寻找到本地的无线网络，如此一来本地无线网络的安全性就会受到影响。为了保护本地无 线网络的安全，我们强烈建议大家关闭这个 SSID 标识符广播功能。

当然，需要提醒各位注意的是，要是非法用户已经知道本地的无线网络 SSID 标识符时，即使我们日 后拒绝无线路由器广播无线网络标识符信息，非法用户也能够偷偷加入到本地的无线网络中来，所以我们在为无线节点设备设置 SSID 名称信息时，尽量要将名称 设置得复杂一些，切忌太脆弱、太简单，确保非法用户不容易猜中本地无线网络的 SSID 标识符名字。

强化无线节点的管理密码

我们知道，一旦无线局域网网络附近的非法用户搜索到本地无线节点后，他们常常会尝试登录到无线节 点的后台管理界面中，去修改它的无线网络参数，要是它们猜中了密码后，那么本地的无线上网参数可能会被非法用户随意修改，从而导致本地无线局域网网络不能 正常工作；更为严重的是，这些非法用户一旦更换了无线节点的后台管理密码时，连本地的网络管理员可能都无法进入到无线节点的后台界面，去管理维护无线上网 设备了。

由于目前很多无线节点设备在默认状态下设置的后台管理密码都比较简单，比方说将密码设置成“admin”、“0000”、“1234”或“aaaa”等等。

要是我们不及时修改这些缺省的后台管理密码就把自己的无线节点设备接入到无线网络中的话,只要有 非法用户利用专业工具得知本地的无线节点设备的生产厂家以及具体型号时，那么本地无线节点设备的管理密码无疑就已经被非法用户掌握了，此时本地无线网络的 安全性就会受到严重威胁。

有鉴于此，我们在将无线节点设备接入到无线网络中之前，必须参照具体的操作说明书，及时登录到该设备的后台管理界面，找到后台管理密码修改选项，并将缺省密码调整成一个非常强壮的密码，确保非法用户无法猜中无线节点的管理密码，从而保证本地无线局域网的工作安全性。

采用加密法保护无线信号

除了上面的几种方法能够保护无线局域网的工作安全性外，还有一种比较有效的保护方法，那就是对无线传输信号进行加密，这种方法往往具有很高的安全防范效果。

当前无线节点设备比较常用的加密方法包括两种，一种是 WEP 加密技术，另外一种就是 WPA 加密技 术。其中 WEP 技术也叫对等保密技术，该技术一般在网络链路层进行 RC4 对称加密，无线上网用户的密钥内容一定要与无线节点的密钥内容完全相同，才能正确 地访问到网络内容，这样就能有效避免非授权用户通过监听或其他攻击手段

来偷偷访问本地无线网络。

正常来说，WEP 加密技术为我们普通用户提供了 40 位、128 位甚至 152 位长度的几种密钥算法 机制。一旦无线上网信号经过 WEP 加密后，本地无线网络附近的非法用户即使通过专业工具窃取到上网传输信号，他们也无法看到其中的具体内容，如此一来本地 无线上网信号就不容易对外泄密了，那么无线局域网的数据发送安全性和接收安全性就会大大提高了。而且 WEP 加密的选用位数越高，非法用户破解无线上网信号 的难度就越大，本地无线网络的安全系数也就越高。

不过 WEP 加密技术也存在明显缺陷，比方说同一个无线局域网中的所有用户往往都共享使用相同的一 个密钥，只有其中一个用户丢失了密钥，那么整个无线局域网网络都将变得不安全。而且考虑到 WEP 加密技术已经被发现存在明显安全缺陷，非法用户往往能够在 有限的几个小时内就能将加密信号破解掉。

因为 WPA 加密技术先天性不足,催生了另外一个更加安全的加密技术-WPA 的出现,这种加密技术可以看作是 WEP 加密技术的增强产品，它比 WEP 加密技术更具安全性和保护性，这种加密技术包含 TKIP 加密方式和 AES 加密方式。

在为无线节点设备设置加密密钥时，我们可以使用两种方式来进行，一种方式比较简单，另外一种方式 则不那么简单。比较简单的方式就是我们可以使用无线节点设备中自带的密钥生成器来自动生成密钥，另外一种方式就是我们采用手工方法选择合适的加密密钥，比 方说我们可以使用字母 A-F 和数字 0-9 的组合来混合设置加密密钥。

要对无线上网信号进行加密时，我们可以先从普通无线工作站中运行 IE 浏览器程序，并在浏览窗口中 输入无线节点设备默认的后台管理地址，之后正确输入管理员帐号名称以及密码，进入到该设备的后台管理页面，单击该页面中的“首页”选项卡，并在对应选项设 置页面的左侧显示区域单击“无线网络”项目，在对应该项目的右侧列表区域，找到“安全方式”设置选项，并用鼠标单击该设置项旁边的下拉按钮，从弹出的下拉 列表中我们可以看到无线节点设备一般能够同时支持“WEP”加密协议和“WPA”加密协议。

选中最常用的“WEP”加密协议，之后选择好合适的身份验证方式，一般无线节点设备都为用户提供 了共享密钥、自动选择以及开放系统这三个验证方式，为了有效保护无线网络传输信息的安全，我们应该在这里选用“共享密钥”验证方式。接着在 “WEP 密码”文本框中正确输入合适的无线网络访问密码，再单击对应设置页面中的“执行”按钮，以便保存好上面的设置操作，最后将无线节点设备重新启动一 下，如此一来我们就在无线节点设备中成功地对本地无线网络进行了加密。

来源： eNet