安全威胁每周警讯

2011/04/09～2011/04/16

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	TROJ_DOWNAD.INF	木马	★★★	→	DOWNAD 蠕虫关联木马
2	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
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	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
6	WORM_ECODE.E-CN	蠕虫	★★★★	↑	E 语言病毒,产生与当前文件夹同名 exe 文件
7	ACM_AGENT.AVGL	脚本病毒	★★	↑	AutoCad 脚本病毒
8	TROJ_SMALL.SMIE	木马	★★★	↑	木马病毒，通过访问恶意站点下载感染或由其他恶意程序下载感染
9	TROJ_LAMEWAR.VTG	木马	★★★	↑	木马病毒，通过访问恶意站点下载感染或由其他恶意程序下载感染
10	WORM_VB.DVP	蠕虫	★★	↑	蠕虫病毒，通过访问恶意站点下载感染。感染该病毒后会在每个盘符下生成 autorun.inf 文件已达到用户在访问磁盘时执行该病毒

系统漏洞信息

MS11-017: 远程桌面客户端中的漏洞可能允许远程执行代码(2508062)

受影响的软件:

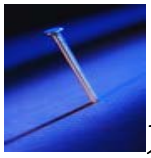
Windows XP

Windows Vista

Windows 7

Windows Server 2003

描述: 请见http://www.microsoft.com/china/technet/security/bulletin/MS11-017.mspx



系统安全技巧

日志记录对于任何一个服务器来说，都是至关重要的。对于 IIS 服务器也不例外。在 Windows7 操作系统中，相比 2003，对于 IIS 日志记录来说有了很大的改进。

IIS 日志

在 Windows7 操作系统中，IIS 日志记录应该视为 ISS 所必需的而不是可选的组件。这主要是因为日志文件对于管理 IIS 服务器来说具有很关键的作用。如在这个 IIS 服务器在受到安全威胁的情况下，可以利用日志文件并对其中包含的内在细节执行排疑式审查。如到 IIS 服务器发生故障后也可以利用这个日志文件中所记录的信息来检查维护过程并识别系统中的问题。笔者这里就给大家介绍一下 Windows7 操作系统中 IIS 日志记录相比 Windows2003 操作系统的一些新特性，并帮助大家部署一种得心应手的日志管理模式。

一、 选择合适的日志记录级别。

在 IIS7.0 版本中，系统管理员可以根据自己的需要选择合适的日志记录级别。如可以在服务器级别上进行日志记录管理，也可以在网站、WEB 应用程序文件或者目录级别上实现它。具体要在哪个级别上实现，主要看系统管理员的需要。不过需要注意的是，其实现级别的不同，所支持的日志文件格式也是不同的。如在“服务器”级别实现的话，其支持的日志格式就只有两种，分别为“W3C”格式与二进制格式。而如果选择“网站”级别上实现日志管理的话，则其支持的日志格式有三种，分别为 IIS、NCSA、W3C 格式。而且系统管理员如果觉得这些格式还不满足的话，可以通过“自定义”的方式来自定义自己需要的格式。所以在选择日志记录级别的时候，除了需要考虑在什么级别上进行日志管理比较方便与安全，同时还需要结合自己喜欢的日志格式。笔者个人喜欢在网站级别上对日志进行管理。因为在一台服务器上，如果只部署 IIS 服务的话，可能比较浪费。也就是说，在同一台服务器上可能有多个应用服务。为了跟其他应用服务与服务器操作系统的日志区分开来，笔者就建议大家在网站级别上进行管理。当然，在哪个级别上进行日志管理，对于日志的内容没有实际性的差异。主要是看服务器的部署以及系统管理员的工作习惯而定。

二、 为日志记录选择合适的格式。

如果选择网站级别来管理日志的话，这个日志的格式有多种选择。最重要的是，系统管理员可以选择 IIS 的日志记录格式。这个 IIS 日志记录格式是基于文本的日志记录。跟 W3C 日志记录格式类似，都是通过 HTTP.SYS 来控制的。不过这个 IIS 日志记录格式是一个核心模式过程。而以前的日志记录都是通过用户模式来管理的。两者之间有比较大的变化。超文本传输协议侦听程序被实现为名为 HTTP.SYS 的内核模式设备驱动程序。HTTP.SYS 是 Windows 网络子系统的一个重要组成部分。在以前的版本中，当在 IIS 中创建网站时，使用 HTTP.SYS 注册站点，然后 HTTP.SYS 将 Web 请求传送到正在运行网站的用户模式进程中。同时 HTTP.SYS 也将响应送回客户端。除了从其内部缓存中检索存储的响应以外，HTTP.SYS 并不处理它所接收到的请求。因此，应用程序特定代码永远不会加载到内核模式中。但是有些系统管理员希望 HTTP.SYS 能够以核心模式运行。此时就需要采用 IIS 日志格式。另外 IIS 是基于文本的日志记录，跟二进制格式的日志记录不同，直接可以通过文本浏览器等工具来查看日志信息。所以阅读起来也更加的方便。

当然，日志文件的格式不同，其所存储的内容都是相同的。所以日志文件的格式并不会影响日志的实际管理价值。不过为了日后管理维护的方便，笔者建立系统管理员最好还是根据自己的工作习惯来选择合适的日志格式。

三、 选择合适的编码格式。

一般情况下，IIS 日志文件的编码格式有两种，分别为 UTF-8 与 ANSI 两种格式。在所有的字符集中，虽然 ANSI 比较有名。但是这个编码格式可以说是专门为英文所设计的。用来存储其他的语言时会出现乱码的情况。如对于汉语就支持的不是很好。为了解决这个问题，特意提出了一种新的编码格式，即 UTF-8。这是一种 UNICODEd 一种变长字符编码。如果 UNICODE 字符由 2 个字节表示，则编码成 UTF-8 很可能需要 3 个字节，而如果 UNICODE 字符由 4 个字节表示，则编码成 UTF-8 可能需要 6 个字节。UTF-8 编码可以通过屏蔽位和移位操作快速读写。字符串比较时 strcmp（）和 wcscmp（）的返回结果相同，因此使排序变得更加容易。字节 FF 和 FE 在 UTF-8 编码中永远不会出现，因此他们可以用来表明 UTF-16 或 UTF-32 文本。 UTF-8 是字节顺序无关的。它的字节顺序在所有系统中都是一样的。

这些字符集的格式对于某些系统管理员来说可能有点深奥。其实系统管理员也不需要了解的这么清楚。只需要明白一个原则。即如果日志中显示的如果都是英文的话，那么采用 ANSI 编码格式也不会有问题。但是如果日志中还会存在其他语言的话，则可能会出现乱码。为此笔者建议，还是采用 UTF-8 的编码格式为好。毕竟，其对于英文的支持力度也是很好的。为此还不如一劳永逸的将其设置为 UTF-8 格式为好。免得以后再日志阅读中遇到乱码的烦恼。

四、 选择合适的日志文件滚动更新机制。

如果将 IIS 的日志记录都保存在一个文件中，显然文件会很长。到时候，查看记录的时候，会很麻烦。为此最好能够将日志文件进行分割，分割成一个个小文件。这方便与后续的查询与阅读。在 Windows7 操作系统的 IIS 日志中，提供了很多的日志文件滚动更新的方法。如可以根据时间来创建新的日志文件。如可以按天、按周或者按月来实现日志文件的滚动更新。一般情况下，按月来更新即可。如果 IIS 服务器访问比较频繁，也可以适当缩短这个日志文件滚动更新的时间间隔。如可以将时间间隔调整为一周或者一天等等。这个时间间隔到底多少为好，主要是看其记录的数量。如果日志记录数量多的话，那么可以适当缩短时间。相反，如果日志记录数量不是很多的话，则可以以月为单位建立新的日志文件。

除了可以根据时间来建立新的日志文件之外，还可以根据日志文件的大小来创建新的日志文件。在 IIS 日志管理器中可以选择“最大文件大小”。然后输入一个合适的尺寸。如此的话，当这个日志文件达到指定的大小之后，系统就会自动对其进行日志切换。不过笔者并不赞同采用这种方法。虽然其可以将重做日志文件控制在一个合理的大小内，但是其会打破其内在的时间联系。到时候，在遇到问题时查询起来会非常的不方便。故笔者还是建立按时间来

对重做日志文件进行分割。

另外管理器还提供另一个有用的选项，即是否要将本地时间用户文件命名与翻滚。这是一个很有用途的选项。选中这个选项后，在系统自动建立的日志文件中就会反映这个时间信息。这对于系统管理员来查找日志文件，能够提供很大的帮助。特别是如果按文件大小来分割重做日志文件的话，一定要选中这个选项，以方便后续的查找。

来源：中关村在线

免责声明