

信息安全漏洞周报

2010年5月10日-2010年5月16日

2010年第19期

本周漏洞基本情况

本周信息安全漏洞威胁整体评价级别为中。

国家信息安全漏洞共享平台(以下简称 CNVD)本周共收集和整理信息安全漏洞 84 个,其中高危漏洞 20 个、中危漏洞 25 个、低危漏洞 39 个。上述漏洞中,可利用来实施远程攻击的漏洞有 80 个。经检测发现,网上已经出现针对“MS PowerPoint 畸形 PPT 文件解析失败漏洞”的零日攻击代码,请广大用户注意做好防护措施。目前,相关厂商已经为 54 个漏洞提供了修补方案,建议用户及时下载补丁更新程序,避免遭受网络攻击。

本周重要漏洞信息

本周, CNVD 整理和发布以下重要安全漏洞信息。

1、Microsoft Outlook Express 和 Windows Mail 存在远程执行代码漏洞

Outlook Express和Windows Mail是Windows操作系统中默认捆绑的邮件和新闻组客户端软件。Outlook Express和Windows Mail客户端所使用的通用库验证特制邮件响应的方式存在整数溢出漏洞,如果用户受骗使用POP3和IMAP邮件协议连接到恶意的服务器并收到畸形的STAT响应就会触发上述溢出漏洞,导致在用户系统上可执行任意代码。微软已于5月11日发布安全公告(MS10-030)修复了该漏洞,建议尚未安装补丁的用户尽快下载使用。

参考链接: <http://www.microsoft.com/china/technet/security/bulletin/MS10-030.msp>

2、Microsoft Visual Basic for Applications 存在远程执行代码漏洞

Microsoft Visual Basic for Applications (VBA) 是微软开发出来在其桌面应用程序中执行通用的自动化 (OLE) 任务的编程语言。在搜索支持 VBA 的文档 (如 Office 文档) 中的 ActiveX 控件时 VBA 所使用的 VBE6.dll 库中的文本解析代码存在单字节栈溢出漏洞。如果主机应用程序打开一个特制文件并将其传递到 VBAruntime, 就会将缓冲区外的值为 0x2E 的单个字节转换为 0x00。成功利用此漏洞的攻击者便可完全控制受影响的系统。微软已于 5 月 11 日发布安全公告 (MS10-031) 修复了该安全漏洞, 建议尚未安装补丁的用户尽快下载使用。

参考链接: <http://www.microsoft.com/china/technet/security/bulletin/MS10-031.msp>

3、Adobe Shockwave Player存在多个远程安全漏洞

Adobe Shockwave Player是专门播放使用Director Shockwave Studio制作的网页的外挂软件。Adobe Shockwave Player播放器存在多个远程安全漏洞，具体漏洞信息为：Adobe Shockwave Player Director文件解析非法偏移远程代码执行漏洞、Director文件分析ATOM size无限循环漏洞、Director文件解析RCSL指针覆盖漏洞、Director文件解析整型溢出漏洞、Adobe Shockwave Player（CVE-2010-1289）未明远程代码执行漏洞、嵌入式字体解析堆溢出漏洞、.dir文件处理整数溢出漏洞、3D对象解析内存破坏漏洞、PAMI块远程代码执行漏洞、Asset Entry解析内存破坏漏洞等。目前厂商已经发布了升级补丁以修复上述安全问题，建议相关用户尽快下载使用。

参考链接：<http://www.adobe.com/support/security/bulletins/apsb10-12.html>

4、Free Download Manager 存在多个缓冲区溢出漏洞

Free Download Manager是一款支持多线程分割下载的工具。Free Download Manager存在多个缓冲区溢出漏洞，可导致应用程序崩溃。具体漏洞信息为："Site Explorer"功能中打开文件夹时、"Site Explorer"功能中打开WEB站点时、解析FTP URLs时、处理重定向时均存在边界错误。目前Free Download Manager 3.0.Build 852已经修复了上述漏洞，建议相关用户尽快下载使用。

参考链接：http://secunia.com/secunia_research/2010-68/

5、MySQL 数据库存在多个安全漏洞

MySQL是一个小型关系型数据库管理系统。MySQL数据库存在多个安全漏洞，远程攻击者可以利用漏洞以应用程序权限执行任意代码。具体漏洞信息为：MySQL在处理COM_FIELD_LIST命令的表格名称参数时没有正确的执行权限检查，对一个表格拥有DELETE或SELECT权限的认证用户可以读取或删除其他表格的内容；服务程序在处理攻击者提交的其大小远超过单个报文规定的最大值的报文时存在一个错误，可锁死服务器状态，造成拒绝服务攻击；COM_FIELD_LIST命令报文处理表名参数缺少正确的边界检查，攻击者通过构建一个超长的表名参数传递给COM_FIELD_LIST，可触发缓冲区溢出。目前MySQL 5.1.47已经修复了上述漏洞，建议相关用户尽快下载使用。

参考链接：<http://secunia.com/advisories/39792/>

小结：本周 Microsoft 发布 5 月份安全公告修复了 Windows 邮件系统和 VBA 中的两个严重漏洞、Adobe 公司发布安全公告 APSB10-12 修复了 Adobe Shockwave Player 的 18 个安全漏洞，此外 Free Download Manager 下载工具、MySQL 数据库等被广泛使用的软件均出现了高危漏洞，这些漏洞可被攻击者利用来进行拒绝服务攻击或远程执行任意代码，对我国网民的上网安全造成严重影响。请广大用户尽快下载相关补丁程序，避免受漏洞的影响。



本周要闻速递

1、Windows 版 Safari 出现一处严重漏洞

5月13日消息，据国外媒体报道，丹麦IT安全公司Secunia和美国计算机应急响应小组(US-CERT)在Windows版苹果Safari浏览器中发现一处严重的零日漏洞。该漏洞会导致计算机受到远程攻击。美国计算机应急响应小组高管表示，利用该漏洞的攻击代码已经被公开发布到互联网上，经证实，Windows版Safari 4.0.5会受到攻击，其他版本也可能受到影响。目前，尽管苹果尚未发布补丁软件修正该漏洞，但用户只需禁用JavaScript代码功能，就不会受到攻击。用户也可以以非管理员权限运行Safari，攻击代码将不会获得运行所需要的权限。

参考链接：<http://www.hackbase.com/news/2010-05-13/35245.html>

2、白宫网站的Drupal代码存在漏洞

白宫网站上开放源码内容管理系统Drupal代码中存在一个漏洞，它可能会导致XSS跨站攻击，并有可能导致攻击者注入登录页面，用恶意脚本获取网站管理密码。漏洞发生在白宫网站Drupal系统中的语境模块，这一发现引人注目，因为白宫网站刚刚向开源团体贡献了自己的源代码，这一漏洞很可能被包含在内并影响其它站点。不过由于要同时符合好几个条件，使用该漏洞实现攻击的难度还是较大，另一方面，由于该漏洞位于模块中，因此Drupal不会协调发布安全修补程序，不过安全人员提供了补丁。

参考链接：<http://www.hackbase.com/news/2010-05-11/35179.html>

3、Web服务器可成为DoS攻击的元凶

一般而言，黑客喜欢到处扫描漏洞然后安插恶意代码的“抓肉鸡”方法来组织僵尸网络，发动拒绝服务(DoS)攻击。但是安全公司Imperva发现，他们多达300台Web服务器组成的“蜜罐系统”最近遭到黑客入侵，服务器被重新配置，并组织针对Google搜索的拒绝服务(DoS)攻击。Web服务器的带宽通常相当大，如果形成一定规模，将可以组成相当可观的攻击流量，一台服务器就可以打出相当于50台PC的量，黑客的主要方法是找出PHP、Web网页上的脆弱部分针对运行Apache、IIS服务器端的系统进行攻击，从而获取控制权。

参考链接：<http://www.hackbase.com/news/2010-05-13/35235.html>

关于 CNVD

国家信息安全漏洞共享平台（China National Vulnerability Database，简称 CNVD）是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库，致力于建立国家统一的信息安全漏洞收集、发布、验证、分析等应急处理体系。

关于 CNCERT

国家互联网应急中心的全称是国家计算机网络应急技术处理协调中心（英文简称是 CNCERT 或 CNCERT/CC）成立于 1999 年 9 月，是工业和信息化部领导下的国家级网络安全应急机构，致力于建设国家级的网络安全监测中心、预警中心和应急中心，以支撑政府主管部门履行网络安全相关的社会管理和公共服务职能，支持基础信息网络的安全防护和安全运行，支援重要信息系统的网络安全监测、预警和处置；国家互联网应急中心在我国大陆 31 个省、自治区、直辖市设有分中心。

网址：www.cert.org.cn

邮箱：vreport@cert.org.cn

电话：010-82990999