

信息安全漏洞周报

2010 年 5 月 31 日-2010 年 6 月 6 日

2010年第22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 56 个,其中高危漏洞 4 个、中危漏洞 7 个、低危漏洞 45 个。上述漏洞中,可利用来实施远程攻击的漏洞有 49 个。经检测发现,网上已经出现针对“Websense Via HTTP 头绕过 Web 过滤漏洞”、“PHP 语言信息泄露漏洞”、“Adobe Flash Player/Adobe Reader/Acrobat 远程代码执行漏洞”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 22 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、PHP 语言存在多个信息泄露漏洞

PHP 是一款流行的网络编程语言。PHP 语言的多个函数存在信息泄露漏洞, 远程攻击者可以利用漏洞获得敏感信息。具体漏洞信息为: PHP 中的 `stripcr()`、`strtr()`、`strip_tags()`、`P setcookie()`、`strtok()`、`wordwrap()`、`str_word_count()`、`str_pad()`、`str_getcsv()`和 `htmlentities()`/`htmlspecialchars()` 函数存在中断处理地址信息泄漏漏洞。目前厂商尚未发布修补方案, 请相关用户随时关注厂商的主页以获取修补补丁或更新版本。

参考链接: <http://php-security.org/category/vulnerabilities/index.html>

2、TCEExam 存在任意文件上传漏洞

TCEExam 是一款开源的在线考试系统, 用于在线试题的生成和管理。TCEExam 的 `admin/code/tce_functions_tcecode_editor.php` 脚本存在安全漏洞, 允许用户向 `webroot` 中的文件夹上传并执行带有任意扩展名的文件。目前厂商尚未发布补丁或升级程序, 建议相关用户随时关注厂商的主页以获取最新版本。

参考链接: <http://secunia.com/advisories/40011/>

3、Novell eDirectory 存在多个漏洞

Novell eDirectory 是一款跨平台的目录服务器。Novell eDirectory 存在多个安全漏洞, 可

被恶意用户利用来实施拒绝服务攻击或未授权获取应用程序执行权限。具体漏洞信息为：在处理畸形verbs时，NDSD存在未明错误，可能导致应用程序崩溃；在dhost.exe处理经特殊构建的GET请求时，存在边界错误，可能导致缓冲区溢出；在对服务器进行某些安全扫描操作时，Dhost存在未明错误，可能导致应用程序崩溃。目前Novell eDirectory 8.8 SP5 Patch 4已经修复了以上漏洞，建议使用该产品的用户尽快下载使用。

参考链接：<http://secunia.com/advisories/40041/>

4、CompleteFTP Server存在两个安全漏洞

CompleteFTP是一款高性能的Windows平台FTP服务器。CompleteFTP存在两个安全漏洞，允许恶意用户绕过安全限制获得系统控制权限。具体漏洞信息为：FTP服务存在输入验证错误，如果攻击者在提交的文件名之前追加".../"序列，则可以下载或替换FTP ROOT目录之外的任意文件；FTP服务存在输入验证错误，允许攻击者通过指定绝对路径更改当前工作目录到文件系统上的任意目录。目前CompleteFTP Server 4.0.3已经修复了以上漏洞，建议受漏洞影响的用户尽快下载使用。

参考链接：<http://secunia.com/advisories/39852/>

5、Google Chrome 存在多个安全漏洞

Google Chrome 是 Google 发布的开源 WEB 浏览器。Chrome 存在多个安全漏洞，如果用户受骗访问恶意网页就可能绕过安全限制或完全入侵用户系统。具体漏洞信息为：Chrome 未能正确地遵循对规范化 URL 的 Safe Browsing 规范；上传事件处理器存在漏洞可能导致伪造 URL 栏；Safe Browsing 交互和拖放功能存在漏洞可能导致内存破坏并执行任意代码；白名单模式的插件拦截器中的漏洞可能导致攻击者绕过安全限制；'drag + drop' 交互功能的漏洞可能导致内存破坏并执行任意代码；扩展上下文中没有正确地执行 JavaScript。目前厂商已经发布了 Google Chrome 5.0.375.55 版本修复了以上安全问题，请相关用户及时下载更新。

参考链接：<http://secunia.com/advisories/39882/>

6、Adobe Flash Player/Adobe Reader/Acrobat存在远程代码执行漏洞

Adobe近日发布了一个安全公告，称Flash Player、Adobe Reader和Acrobat中存在一个严重安全漏洞，该漏洞(CVE-2010-1297)可导致应用程序崩溃或泄露系统控制权限，Flash Player 10.1 Release Candidate不受此漏洞影响，用户可下载使用。Adobe表示已经接到有黑客利用该漏洞进行攻击的报告，目前Adobe尚未提供官方修补方案，用户可采取重命名或删除Adobe Reader/Acrobat 9.x下的authplay.dll文件来暂时规避此漏洞带来的风险。建议广大Adobe产品用户尽快采取防范措施。

参考链接：<http://www.cert.org.cn/articles/bulletin/common/2010060725012.shtml>

小结：本周爆出的 PHP 语言信息泄露漏洞对使用 PHP 语言开发的应用软件构成严重安全威胁。Adobe 系列产品远程代码执行漏洞，不仅影响面广，几乎影响所有的操作系统平台；而且可导致系统完全控制权泄露，危险程度高，目前已经有黑客利用此漏洞进行攻

击。Google Chrome 浏览器、TCExam 在线考试系统、Novell eDirectory 目录服务器、CompleteFTP 服务器等漏洞，也对国内网民的上网安全构成一定影响。请广大用户尽快采取防范或修补更新措施，避免引发漏洞相关的安全事件。

本周重要漏洞修补信息

本周，CNVD 整理和发布以下重要安全修补信息。

1、Bftpd 的安全漏洞补丁包

Bftpd 是一款小型的 FTP 服务器。Bftpd 处理匿名登录时可能会忽略配置文件中所指定的 ROOTDIR 选项，从而允许用户绕过限制获得对系统任意文件或目录的读写访问。Bftpd 已于 6 月 2 日发布相关补丁包，修复了该安全漏洞。建议用户尽快下载补丁程序修复漏洞，以避免发生漏洞被利用事件。

补丁下载链接：<http://bftpd.sourceforge.net/news.html>

本周要闻速递

1、Adobe 产品漏洞影响广泛

北京时间 6 月 6 日消息，Adobe 在日前发布的重大软件安全公告中称，公司旗下 Flash Player 和 Adobe Reader 两款产品存在安全隐患，黑客可以利用该漏洞远程控制安装了上述软件的计算机。此漏洞影响的软件包括：Adobe Flash Player 10.0.45.2，9.0.262，以及早期支持 Windows、Macintosh、Linux 和 Solaris 操作系统的 10.0.x 和 9.0.x 版本；Adobe Reader 和 Acrobat 9.3.2 以及早期支持 Windows、Macintosh 和 UNIX 操作系统的 9.x 版本。Adobe PDF 阅读器和 Acrobat 8.x 尚不能证实是否会受此安全缺陷的影响。Adobe 公司表示，Flash Player 的 10.1 版本已确认不存在该缺陷。

参考链接：<http://www.hackbase.com/news/2010-06-07/35722.html>

2、帝国（EmpireCMS）6.0 存在多个跨站漏洞

帝国软件是一家专注于网络软件开发的科技公司，其主营产品“帝国网站管理系统（EmpireCMS）”是目前国内应用广泛的 CMS 程序。目前 EmpireCMS 程序已经广泛应用在国内数十万家网站，覆盖国内上千万上网人群，并经过上千家知名网站的严格检测，被称为国内最稳定的 CMS 系统。但是，目前发现帝国（EmpireCMS）6.0 的 /search/keyword/index.php 存在多个跨站漏洞，厂商尚未提供补丁或升级程序。

参考链接：<http://www.hackbase.com/news/2010-06-05/35701.html>

3、苹果某些软件被爆含有间谍软件

为 Mac 系统提供安全和隐私软件的厂商 Intego 警示说，一些 Mac 软件含有间谍软件。Macworld 已经取得了存在该间谍软件的初步软件列表。该间谍软件被称为 OSX/OpinionSpy，它是 2008 年出现的 Windows 间谍软件的变种。OSX/OpinionSpy 弹出一

个对话框，以市场调查的名义欺骗用户，取得 admin 密码，安装“PremierOpinion”进程以 root 身份运行，在 8254 端口打开 http 后门，扫描所有本地和网络驱动卷，向 Safari, Firefox 以及 iChat 中注入恶意代码，窃取包含电子邮件地址等信息的加密数据以及用户名，密码，信用卡号码等个人数据。OSX/OpinionSpy 可以自动升级并通过 Mac OS 自启动，即使卸载宿主程序，它依然在 Mac 中存在。Intego 建议用户将安全软件 VirusBarrier X5 和 X6 的威胁库升级到 2010 年 5 月 31 日，即可清除该间谍软件。

参考链接：<http://www.hackbase.com/news/2010-06-02/35627.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