

信息安全漏洞周报

2010年7月5日-2010年7月11日

2010年第26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 59 个,其中高危漏洞 15 个、中危漏洞 14 个、低危漏洞 30 个。上述漏洞中,可利用来实施远程攻击的漏洞有 57 个。经检测发现,网上已经出现针对“Wiki Web Help 'getpage.php' SQL 注入漏洞”、“Linux Kernel 'btrfs'文件权限安全绕过漏洞”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 33 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、Adobe Reader/Acrobat 存在多个安全漏洞

Adobe Reader/Acrobat是Adobe公司开发的PDF文档阅读/编辑软件。Adobe Reader/Acrobat存在多个安全漏洞,攻击者可利用漏洞实施特定代码执行、跨站脚本攻击、拒绝服务攻击等恶意活动。具体漏洞包括: Adobe Acrobat/Reader内容解析远程缓冲区溢出漏洞、Adobe Acrobat/Reader CLOD远程内存破坏漏洞、Adobe Reader cooltype.dll内存破坏漏洞、Adobe Acrobat/Reader 'AcroForm.api' GIF图像远程代码执行漏洞、Adobe Acrobat/Reader 'pushstring'和'debugfile'远程代码执行漏洞、Adobe Acrobat/Reader 'newclass' Flash内容远程代码执行漏洞、Adobe Acrobat/Reader 'newfunction'远程代码执行漏洞、Adobe Acrobat/Reader 'AcroForm.api'远程代码执行漏洞。目前Adobe已经发布更新程序修复了上述漏洞,建议相关用户尽快下载更新。

参考链接: <http://www.cnvd.org.cn/vulnerability/CNVD-2010-01290>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01289>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01288>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01287>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01286>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01285>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01284>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01283>

2、KVIrc 存在两个安全漏洞

KVIrc 是一款功能强大的 IRC 客户端软件。KVIrc 存在两个安全漏洞，远程攻击者可利用漏洞实施拒绝服务攻击。具体漏洞信息为：KVIrc DCC 请求存在多个格式串漏洞，远程攻击者可通过提交经特殊构建的格式串触发内存破坏，导致应用程序崩溃；KVIrc DCC 请求存在目录遍历漏洞，KVIrc 不能正确处理用户提交的经特殊构造的 DCC 请求，远程攻击者可通过目录遍历攻击覆盖本地文件，导致应用程序崩溃。目前厂商已经发布更新程序修复了上述漏洞，建议相关用户尽快下载更新。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01298>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01297>

3、LibTIFF应用库存在多个安全漏洞

LibTIFF是负责对TIFF图象格式进行编码/解码的应用库。LibTIFF应用库存在多个安全漏洞，攻击者可利用漏洞对应用程序执行拒绝服务攻击。具体漏洞包括：LibTIFF库忽略文件标签导致拒绝服务漏洞；LibTIFF库TIFFReadDirectory函数拒绝服务漏洞；LibTIFF库TIFFRGBImageGet函数拒绝服务漏洞；LibTIFF库OJPEGReadBufferFill()函数空指针引用拒绝服务漏洞；LibTIFF库TIFFExtractData宏拒绝服务漏洞。目前厂商已经发布升级补丁修复上述漏洞，建议相关用户尽快下载使用。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01323>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01322>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01321>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01320>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01319>

4、Google Chrome 5.0.375.99 之前版本存在多个安全漏洞

Google Chrome是Google公司开发的开源WEB浏览器。Chrome 5.0.375.99之前版本存在多个安全漏洞，攻击者诱使用户访问恶意网页后，可实施拒绝服务攻击或获得用户系统控制权。具体漏洞信息为：在使用WebGL时Chrome中可能出现越界读访问错误；Chrome没有正确地隔离沙盒中的IFRAME元素；无效的SVG文档可能触发内存破坏；Chrome中Unicode双向算法实现中的错误可能导致内存破坏；Chrome CSS实现没有正确地渲染样式，可能触发内存破坏；Chrome没有正确的实现modal对话框，可能导致拒绝服务攻击。目前Google已经发布升级补丁修复了上述漏洞，建议相关用户尽快下载使用。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01327>

5、Sandbox 存在多个安全漏洞

Sandbox是一套采用PHP编写的个人站点工具包。Sandbox存在多个输入验证漏洞，远程攻击者可利用漏洞进行SQL注入攻击、获取敏感信息、上传任意文件等。目前iguanadons.net Sandbox 2.0.4版本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://www.cnvd.org.cn/vulnerability/CNVD-2010-01335>

小结: 本周 CNVD 收集的漏洞信息中, Adobe Reader /Acrobat、Google Chrome5.0.375.99 之前版本存在的多个严重漏洞,可被攻击者利用来执行特定代码或拒绝服务攻击; Sandbox、LibTIFF 应用库、KVirc 客户端软件出现的严重漏洞,对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、Panda 多个产品'RKPavProc.sys' IOCTL 请求特权提升漏洞的补丁

熊猫卫士是 Panda 软件公司在中国推出的系列反病毒产品。Panda 发布安全公告,修复了熊猫卫士杀毒软件 RKPavProc.sys 驱动 IOCTL 请求内核权限提升漏洞,即多个熊猫杀毒软件产品所使用的 RKPavProc.sys 内核驱动没有正确地处理用户所发送的 IOCTL 请求,本地用户可以通过执行恶意程序触发空指针引用或栈溢出,导致内核崩溃或执行任意内核代码。

补丁下载链接: <http://www.cnvd.org.cn/patch/593>

本周要闻速递

1、Chrome 扩展曝严重安全漏洞

近日, Chrome 扩展被曝存在严重安全漏洞,黑客可通过任意一个扩展得到用户登陆网站的用户名与密码。曝光这个漏洞的程序员通过在扩展中加入一段 jQuery 代码来抓取用户的登陆信息,然后将登陆信息通过电子邮件发送给自己。他宣称已经测试了这个扩展,并可以成功得到 Twitter、Gmail、FaceBook 以及其他网站的用户名与密码。

参考链接: <http://www.hackbase.com/news/2010-07-12/36404.html>

2、Skype 安全协议遭破解

美国科技博客 TechCrunch 表示,有人宣称已利用反向工程技术破解 Skype 专有加密协议。若该消息得到证实,这意味着 Skype 悉心构筑的安全措施将失效。Skype 系统被入侵的后果目前还不清楚,但黑客至少可以利用反向工程获知更多信息,并利用这些信息。Skype 表示,目前根本不存在安全问题,加密协议被破解事件正处在调查当中。

参考链接: <http://www.hackbase.com/news/2010-07-11/36392.html>

3、全球最大 BT 网站曝安全漏洞

7月9日消息,据外电媒体报道,全球最大 BT 网站海盗湾(Pirate Bay)服务器存在安全漏洞,导致 400 多万用户的个人信息被泄露。海盗湾因服务器存在漏洞被黑客攻击,同时黑客表示已可入侵存储用户信息的数据库。阿根廷黑客查·卢索和另外两名同事发现了多

个 SQL 注入漏洞，允许黑客访问海盗湾的用户数据库。之后，黑客可以查看、修改、创建或删除所有用户的信息，包括用户名、电子邮件、用户上传的种子，以及正在下载的用户数量和名称等。海盗湾对该安全漏洞十分重视，目前该网站已经无法正常访问，页面提示：“网站升级，数据库正在备份，将很快恢复正常。”

参考链接：<http://www.hackbase.com/news/2010-07-09/36350.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