

信息安全漏洞周报

2010年4月5日-2010年4月11日

2010年第14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洞44个,其中高危漏洞11个、中危漏洞12个、低危漏洞21个。上述漏洞中,可利用来实施远程攻击的漏洞有31个。经检测发现,网上已经出现了针对“Windows平台下的Apple iTunes存在本地权限提升漏洞”、“Uiga Proxy存在安全漏洞”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30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、Windows平台下的Apple iTunes存在本地权限提升漏洞

Apple iTunes是一款流行的媒体播放器。Windows平台下的Apple iTunes在安装过程中会在%ALLUSERSPROFILE%\Application Data\路径的目录上安装并执行部分文件。由于默认允许任意用户向此路径写入文件,恶意用户可利用漏洞在安装前后创建带有特定文件名的恶意文件,并以SYSTEM权限执行。目前厂商已经发布了升级补丁以修复这个安全问题,请使用该软件的用户及时到厂商的主页下载。

参考链接: <http://secunia.com/advisories/39135/>

2、Uiga Proxy存在安全漏洞

Uiga Proxy是一款允许用户在防火墙/代理服务器后方访问受限WEB站点的代理服务器。Uiga Proxy在给'include/template.php'脚本传递"content"参数时,未进行正确校验。远程攻击者可以利用漏洞,导致敏感信息泄漏或以WEB权限执行任意PHP代码。目前厂商尚未提供解决方案。

参考链接: <http://secunia.com/advisories/39313/>

3、Mozilla Firefox存在多个安全漏洞

Mozilla Firefox是一款开放源代码的网页浏览器。其存在的多个安全漏洞可允许远程攻

击者以应用程序权限执行任意指令。具体漏洞包括：Mozilla Firefox DOM节点移动释放后使用漏洞、Firefox window.navigator.plugins对象悬空指针任意代码执行漏洞、Mozilla Firefox nsTreeSelection EventListener任意代码执行漏洞、Mozilla Firefox nsTreeContentView悬空指针任意代码执行漏洞、Mozilla Firefox图形SRC重定向mailto: URL启动email编辑器漏洞、Mozilla Firefox XMLHttpRequestSpy任意代码执行漏洞、Mozilla Firefox强制URL拖放特权提升漏洞、Mozilla Firefox多个内存破坏漏洞、Mozilla Firefox XML解析绕过安全漏洞。供应商已经发布了安全公告及补丁，请用户及时下载更新。

参考链接：<http://www.mozilla.org/security/announce/2010/mfsa2010-17.html>

4、Linux Kernel 存在多个设计错误漏洞

Linux是一款开放源代码的操作系统。Linux Kernel存在多个设计错误漏洞,允许本地攻击者利用漏洞使系统崩溃。具体漏洞包括：Linux Kernel "cifs_create()"空指针引用漏洞、Linux Kernel GFS/GFS2本地拒绝服务漏洞、Linux Kernel NFS启动加载'symlinks'拒绝服务漏洞、Linux Kernel 'l2cap_config_rsp()'远程拒绝服务漏洞、Linux Kernel蓝牙sysfs文件本地特权提升漏洞、Linux Kernel nfs_wait_on_request函数本地拒绝漏洞、Linux Kernel net/ipv4/tcp_input.c释放后使用漏洞、Linux Kernel 'tipc'模块本地拒绝服务漏洞。目前厂商尚未发布升级补丁，请用户随时关注厂商的主页以获取最新版本。

参考链接：<https://bugzilla.redhat.com/duplicates.cgi>

5、Zip Unzip 存在边界条件错误漏洞

Zip Unzip是一款免费的解压缩工具。Zip Unzip处理压缩文档中包含超长路径的文件时存在边界错误，攻击者可通过诱使用户解析其特殊构建的ZIP文档，来触发基于栈的缓冲区溢出。成功利用漏洞可以以应用程序权限执行任意指令。目前厂商尚未发布升级补丁，请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/39280/>

小结：本周 CNVD 所整理的漏洞信息中，Apple 媒体播放器、Uiga Proxy 代理服务器、Mozilla Firefox 浏览器、Linux 操作系统和 Zip Unzip 解压缩工具等均出现了严重漏洞。其中漏洞 1、2 网上已经出现零日攻击代码，严重影响了我国网民的上网安全，请广大用户注意采取安全防范措施，尽快下载相关补丁程序。

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、libpng 多个漏洞安全补丁包

4 月 11 日，Debian 发布安全公告（DSA-2032-1）及相应补丁，修复了 Libpng png_decompress_chunk()函数拒绝服务漏洞和 Libpng 库 1 位隔行图形信息泄露漏洞。

补丁下载链接：<http://www.debian.org/security/2010/dsa-2032>

2、MIT Kerberos kadmind server_stubs.c 远程拒绝服务漏洞补丁包

4月11日，Debian 发布安全公告（DSA-2031-1）及相应补丁，修复了 MIT Kerberos kadmind server_stubs.c 远程拒绝服务漏洞。

补丁下载链接：<http://www.debian.org/security/2010/dsa-2031>

本周要闻速递

1、Mozilla 将修复 Firefox 遗留 8 年的漏洞

据报道，Mozilla 正计划修复 Firefox 浏览器中存在于 8 年的错误。该错误存在于 Firefox 浏览器的层叠样式表（CSS）中，研发人员可以很容易的从 CSS 中获得用户已访问过的列表清单。Mozilla 基金会准备用以下三种方法来修补该问题：1）通过改变已访问链接的风格，使得已访问链接很难被其他人筛选出来；2）尽量缩小已访问链接和未访问链接之间的展示时间差异；3）关闭使用 Java 脚本函数调用浏览器历史数据的功能。但截至目前，Mozilla 基金会尚未给出解决这一问题补丁包的具体时间。

参考链接：<http://www.cert.org.cn/articles/news/common/2010040724908.shtml>

2、Java 运行环境存在重大安全漏洞

安全研究人员在研究 Java 运行环境时发现一个重大漏洞，远程攻击者可利用最终用户机器上的 Java 最新版本来执行恶意代码。该问题出在 Java Web Start 的组件上，它可以通过 IE、Firefox 和其它浏览器与应用程序被调用，攻击者可通过这些应用锁打开的特别设计后的网站传输恶意指令。目前相关厂商尚未为它发布补丁，暂时的修补程序只适用于 IE 和 Firefox 浏览器。

参考链接：<http://www.cert.org.cn/articles/news/common/2010041224918.shtml>

3、Facebook 新漏洞可致用户数据失窃

安全研究人员发现 Facebook 平台存在严重的安全漏洞，该漏洞允许恶意网站在用户不知情的情况下窃取用户的信息、照片等个人数据，并会导致用户邮件遭窃。据研究人员称该漏洞可能已存在一年之久，但还没有证据表明该安全漏洞遭到滥用。目前该漏洞尚未被修复。

参考链接：<http://www.hackbase.com/news/2010-04-12/34693.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