

信息安全漏洞周报

2010 年 12 月 06 日-2010 年 12 月 12 日

2010 年第 48 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低。

国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 103 个，其中高危漏洞 29 个、中危漏洞 22 个、低危漏洞 52 个。上述漏洞中，可利用来实施远程攻击的漏洞有 93 个。经跟踪发现，网上已经出现针对“Enano CMS SQL 注入漏洞”、“Microsoft Internet Explorer CSS 解析远程拒绝服务漏洞”、“Freefloat FTP Server 'USER' 命令远程缓冲区溢出漏洞”等的零日攻击代码，请使用相关产品的用户注意做好防护措施。本周收录的安全漏洞中，已有 80 个漏洞由厂商提供了修补方案，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、Google Chrome 存在多个安全漏洞

Google Chrome 是一款开源的 WEB 浏览器。本周，Google Chrome 出现多个安全等级为“高”的漏洞，攻击者可以利用这些漏洞破坏内存或进行拒绝服务攻击。CNVD 本周收录的 Google Chrome 漏洞包括：Google Chrome XPath 处理存在释放后使用漏洞、Google Chrome 鼠标拖拉时间处理存在释放后使用漏洞、Google Chrome SVG 动画处理存在释放后使用漏洞、Google Chrome 特权扩展处理存在漏洞、Google Chrome 畸形视频数据中的索引存在漏洞、Google Chrome WebM 视频支持存在未明漏洞、Google Chrome HTTP 代理验证存在未明漏洞、Google Chrome 历史处理存在释放后使用漏洞、Google Chrome 存在使应用程序崩溃漏洞、Google Chrome 存在使 HTML5 数据库崩溃漏洞、Google Chrome 存在未明漏洞。目前，Google 已经发布了补丁程序修复这些漏洞，CNVD 建议用户及时下载更新，避免引发此类漏洞相关的安全事件。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03147>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03146>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03145>

[http://www.cnvd.org.cn/vulnerability/ CNVD-2010-03144](http://www.cnvd.org.cn/vulnerability/CNVD-2010-03144)
<http://www.cnvd.org.cn/vulnerability/ CNVD-2010-03143>
<http://www.cnvd.org.cn/vulnerability/ CNVD-2010-03142>
<http://www.cnvd.org.cn/vulnerability/ CNVD-2010-03141>
<http://www.cnvd.org.cn/vulnerability/ CNVD-2010-03140>
<http://www.cnvd.org.cn/vulnerability/ CNVD-2010-03139>
<http://www.cnvd.org.cn/vulnerability/ CNVD-2010-03138>
<http://www.cnvd.org.cn/vulnerability/ CNVD-2010-03137>

2. Apple QuickTime 存在多个安全漏洞

Apple QuickTime 是 Apple 公司发布的多媒体播放器软件。本周, CNVD 收录了 Apple QuickTime 的多个“高危”漏洞。具体漏洞包括: Apple QuickTime 存在文件系统权限问题可导致本地信息泄漏漏洞、Apple QuickTime 视频文件整数溢出远程代码执行漏洞、Apple QuickTime FlashPix 图像(CVE-2010-3801)内存破坏远程代码执行漏洞、Apple QuickTime (CVE-2010-3802) QTVR 文件内存破坏远程代码执行漏洞、Apple QuickTime Track 头(tkhd)原子堆缓冲区溢出漏洞、Apple QuickTime 解析.pict 文件中的 directBitsRect 记录存在漏洞、Apple QuickTime 自定义压缩算法实现存在漏洞。攻击者可以利用这些漏洞以用户权限执行任意指令。目前, Apple 已经发布了这些漏洞的补丁更新, CNVD 建议用户及时下载更新, 避免引发此类漏洞相关的安全事件。

参考链接: <http://www.cnvd.org.cn/vulnerability/CNVD-2010-03176>
<http://www.cnvd.org.cn/vulnerability/ CNVD-2010-03175>
<http://www.cnvd.org.cn/vulnerability/ CNVD-2010-03174>
<http://www.cnvd.org.cn/vulnerability/ CNVD-2010-03173>
<http://www.cnvd.org.cn/vulnerability/ CNVD-2010-03172>
<http://www.cnvd.org.cn/vulnerability/ CNVD-2010-03171>
<http://www.cnvd.org.cn/vulnerability/ CNVD-2010-03170>

3、Mozilla 产品存在多个安全漏洞

本周, Mozilla 的 Firefox 和 SeaMonkey 产品出现了多个安全漏洞。Firefox 是 Mozilla 的一款 WEB 浏览器, SeaMonkey 是 Mozilla 所发布的新闻组客户端。CNVD 本周收录的漏洞包括: Mozilla Firefox/SeaMonkey 存在缓冲区溢出漏洞、Mozilla Firefox/SeaMonkey 存在不正确计算子内容的索引漏洞、Mozilla Firefox 通过 window.open()打开时存在正确校验漏洞、Mozilla Firefox 处理畸形 OpenType 字体存在漏洞、Mozilla Firefox/SeaMonkey 存在错误的安全规则创建插件对象漏洞、Mozilla Firefox/SeaMonkey 存在以 chrome 特权执行任意 JavaScript 漏洞、Mozilla Firefox/SeaMonkey 存在脚本注入漏洞等。攻击者可以利用这些漏洞实施执行任意代码和进行注入 WEB 脚本等攻击, 造成用户应用程序崩溃或权限被获取。目前厂商已经发布了补丁程序修复了这些漏洞, CNVD 建议广大 Mozilla 用户及时下载更新, 避免引发此类漏洞的相关安全事件。

参考链接: <http://www.cnvd.org.cn/vulnerability/CNVD-2010-03240>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03239>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03237>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03235>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03233>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03232>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03231>

4、Linux Kernel 存在多个安全漏洞

Linux Kernel 是开源操作系统 Linux 所使用的内核。本周, Linux Kernel 出现了多个安全漏洞, 攻击者可以利用这些漏洞获取敏感信息或造成系统崩溃。CNVD 本周收录的相关漏洞包括: Linux Kernel 'install_special_mapping()'本地安全绕过漏洞、Linux Kernel 'AF_ECONET'协议空指针引用拒绝服务漏洞、Linux Kernel IGB Panic VLAN 报文远程拒绝服务漏洞。其中, “Linux Kernel IGB Panic VLAN 报文远程拒绝服务漏洞”的安全等级为“高”。除“Linux Kernel 'AF_ECONET'协议空指针引用拒绝服务漏洞”外, 厂商已经发布了其余漏洞的补丁, CNVD 建议用户及时下载使用, 避免引发此漏洞的相关安全事件。

参考链接: <http://www.cnvd.org.cn/vulnerability/CNVD-2010-03238>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03234>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03154>

5、Pandora FMS 存在多个安全漏洞

Pandora FMS 是一个用来监测网站的各种活动的开源软件。本周, Pandora FMS 出现多个“高危”漏洞。CNVD 收录的漏洞包括: Pandora FMS extras/pandora_diag.php 文件 PHP 远程文件包含漏洞、Pandora FMS 目录遍历漏洞、Pandora FMS ajax.php 文件代码注入漏洞、Pandora FMS SQL 注入漏洞、Pandora FMS 认证绕过和输入验证错误漏洞。其中“Pandora FMS SQL 注入漏洞”为 0day 漏洞, 互联网上已经出现针对 Pandora FMS 3.1.1 之前版本的漏洞攻击程序。攻击者可以利用这些漏洞执行任意代码。目前, 厂商已经发布漏洞的补丁程序, CNVD 建议用户及时下载使用, 避免引发此漏洞的相关安全事件。

参考链接: <http://www.cnvd.org.cn/vulnerability/CNVD-2010-03190>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03189>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03185>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03182>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03166>

小结: 本周, Google、Linux、Apple、Mozilla 等厂商的产品均出现了安全漏洞, 对国内用户的信息安全和互联网网络安全构成较为严重的威胁, 请使用上述软件的相关机构和个人及时采取安全防范措施。

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、Winamp 发布升级程序修补了多个安全漏洞

Winamp 是一款被广泛使用的音乐播放软件。本周，Winamp 出现了多个安全漏洞，攻击者利用这些漏洞可以实施执行任意代码攻击。CNVD 已收录漏洞的相关升级修补程序，请广大用户及时下载更新，避免引发漏洞相关的安全事件。

补丁下载链接：<http://www.cnvd.org.cn/patch/1975>
<http://www.cnvd.org.cn/patch/1977>
<http://www.cnvd.org.cn/patch/1978>
<http://www.cnvd.org.cn/patch/1979>

本周要闻速递

1. 微软称 IE 保护模式被绕过并非漏洞

上周，Verizon Business 发布了一份报告，详细列出了他们发现的“逃离微软 IE 保护模式”。Verizon Business 指出，IE7 和 IE8 的保护模式都可以被绕过，攻击者能提高其用户权限。微软日前对此作出了回应，微软一位主管发表了以下声明：“这份报告中发现的问题并不是一个漏洞，它只是绕过安全防护的一种方法。如果想要使用这种方法，攻击者首先需要利用受攻击计算机上一个未打补丁的漏洞。”Bryant 建议用户升级至最新的 IE 版本，以便获得更高的安全性免于受到恶意行为的攻击。

参考链接：<http://tech.sina.com.cn/s/2010-12-09/09494962988.shtml>

2. 美国改造互联网接入系统防止敏感信息被盗取

为了遏制黑客袭扰不断升级的现象，美国联邦政府实施了代号为“爱因斯坦”的网络安全工程。据悉，整个项目将持续数年时间才能完成。届时，美国联邦政府设在互联网上的 2400 多处“接入点”将处于严密保护之下，从而防止黑客盗取各类敏感信息。美国国土安全部表示，本次接受改造的互联网接入系统不涉及就军方网站。未来美联邦政府雇员的所有网络活动(如浏览网页和收发电子邮件)都将通过特别打造的安全网络进行。不过，此举也引发了一些人的顾虑，并担心它可能会侵害联邦政府雇员的隐私权。

参考链接：<http://b2b.toocle.com/detail--5541702.html>

3. 浏览器漏洞让网站可窃取网友浏览记录

根据美国加州大学圣地亚哥分校一份 JavaScript 网页程序隐私资料流向验证研究报告显示，Alexa 排行前五万大的网站中，有 485 个网站利用浏览器漏洞，未经使用者同意就读取浏览记录。这 485 个网站中共有 63 个网站会把浏览记录上传，其中 46 个网站积极运用这些记录，其他 17 个网站则不确定用途。YouPorn.com、TwinCities.com、Charter.net 等网

站均会读取使用者的浏览纪录，幸好新一代的浏览器已经对此免疫，苹果的 Safari 及 Google 的 Chrome 这两种浏览器最新版本已经修补这个问题，Firefox 则要等到 4.0 版，IE 只能在 “InPrivate 浏览” 匿踪模式下才能避免被读取浏览记录。FireFox 的 NoScript 则可以关闭大部分的 JavaScript 程序，仅让授权过的程序执行。

参考链接：<http://www.enet.com.cn/article/2010/1208/A20101208794248.shtml>

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