

信息安全漏洞周报

2011 年 3 月 14 日-2011 年 3 月 20 日

2011 年第 11 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 100 个，其中高危漏洞 16 个、中危漏洞 28 个、低危漏洞 56 个。上述漏洞中，可利用来实施远程攻击的漏洞有 87 个。网上已经出现针对“Adobe Flash Player 'SWF'文件远程内存破坏漏洞”、“Windows Movie Maker '.avi'文件远程缓冲区溢出漏洞”和“iPhone/iPod Touch checkview 目录遍历漏洞”等漏洞的零日攻击代码，请使用相关产品的用户注意做好防护措施。本周收录的漏洞中，已有 62 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、Apple 产品安全漏洞

本周，Apple 的 IOS 操作系统、Safari 浏览器、Webkit 浏览器引擎等多个产品均出现了安全漏洞。远程攻击者可以利用漏洞窃取代码执行权限或发起拒绝服务攻击。CNVD 收录的具体漏洞包括：Apple IOS Mobile Safari 任意代码执行漏洞、Apple Safari WebKit 任意代码执行漏洞、Apple IOS WebKit 任意代码执行漏洞、Apple TV IPv6 网络实现无状态地址自动配置功能用户追踪漏洞、Apple IOS 网络实现无状态地址自动配置功能用户追踪漏洞、iPhone/iPod Touch checkview 目录遍历漏洞。其中，“Apple IOS Mobile Safari 任意代码执行漏洞”、“Apple Safari WebKit 任意代码执行漏洞”和“Apple IOS WebKit 任意代码执行漏洞”的综合评级为“高危”。目前，互联网上已经出现了针对“iPhone/iPod Touch checkview 目录遍历漏洞”的攻击代码，主要影响 iPhone/iPod Touch checkview 1.1 版本。除“Apple Safari WebKit 任意代码执行漏洞”和“Apple IOS Mobile Safari 任意代码执行漏洞”外，Apple 已经提供了补丁程序修复其余漏洞，CNVD 提醒广大用户及时下载更新，避免引发漏洞相关的安全事件。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04735>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04733>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04732>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04714>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04711>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04653>

2、Linux Kernel 安全漏洞

Linux Kernel 是开源操作系统 Linux 所使用的内核。本周，Linux Kernel 被披露存在多个安全漏洞。本地攻击者可以利用漏洞获得敏感信息或者导致拒绝服务。CNVD 收录的漏洞包括：Linux Kernel 'fs/partitions/osf.c'信息泄露漏洞、Linux Kernel "ldm_frag_add()"缓冲区溢出漏洞、Linux Kernel 'drivers/char/tpm/tpm.c'信息泄露漏洞、Linux Kernel I/O-Warrior USB 设备堆缓冲区溢出漏洞、Linux 内核请求处理'cm.c'拒绝服务漏洞。其中，“Linux Kernel "ldm_frag_add()"缓冲区溢出漏洞”的综合评级为“高危”，厂商尚未发布此漏洞的补丁程序。对于其余漏洞，厂商已经提供了补丁程序，CNVD 提醒广大用户及时下载更新，避免引发漏洞相关的安全事件。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04722>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04736>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04663>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04638>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04637>

3、SAP 产品安全漏洞

SAP Crystal Reports Server 是一款报表解决方案，SAP NetWeaver 是一款业务套件解决方案。本周，SAP 的产品出现了多个安全漏洞，利用这些漏洞，远程攻击者可以获得敏感信息或劫持目标用户会话。CNVD 收录的漏洞包括：SAP Crystal Reports Server"DocName"和"Label"参数漏洞、SAP Crystal Reports Server 参数输入漏洞、SAP GUI DLL 装载任意代码执行漏洞、SAP Crystal Reports Server"defTar"参数漏洞、SAP Crystal Reports Server"analyticToken"参数漏洞、SAP Crystal Reports Server"Sel"参数漏洞、SAP Crystal Reports Server"swf"参数漏洞、SAP Crystal Reports Server 多个参数漏洞。目前，厂商已经提供了补丁程序修复上述漏洞，CNVD 提醒广大用户及时下载更新，避免引发漏洞相关的安全事件。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04677>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04676>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04675>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04674>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04673>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04672>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04671>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04670>

4、Adobe Flash Player 'SWF'文件远程内存破坏漏洞

本周，Adobe Flash Player 被披露存在一个综合评级为“高危”的“Adobe Flash Player 'SWF'文件远程内存破坏零日漏洞”。攻击者通过在微软 Excel (.xls) 表格文件中嵌入特定构造的 Flash (.swf) 文件，诱使用户打开.xls 文件发起攻击（通常可以把.xls 文件作为邮件附件发送）。Adobe 已经确定 Adobe Flash Player、Adobe Reader 和 Acrobat 产品中都存在此严重的安全问题。这个漏洞存在于以下平台版本：Windows、Mac、Linux 和 Solaris 平台最新 Adobe Flash Player 10.2.152.33 版本以及更早版本。目前 Adobe 官方尚未对此漏洞发布补丁或相关更新程序，CNVD 提醒广大用户随时关注厂商主页以获取最新版本，避免引发漏洞相关的安全事件。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04654>

5、Google 产品安全漏洞

本周，Google Chrome 和 Chrome OS 出现了两个综合评级为“高危”的安全漏洞。Google Chrome 是一款开放源代码的 WEB 浏览器，Chrome OS 是一款基于 PC 的操作系统。CNVD 收录的 Google 漏洞包括：Google Chrome 应用程序未明漏洞、Google Chrome 样式处理内存破坏漏洞。攻击者利用漏洞进行恶意攻击，在受影响的程序中执行任意代码。目前，Google 已经发布补丁修复了这些漏洞，CNVD 提醒广大用户及时下载更新，避免引发漏洞相关的安全事件。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04723>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04659>

小结：本周，Adobe Flash Player 被披露存在一个“高危”的“Adobe Flash Player 'SWF'文件远程内存破坏零日漏洞”，攻击者可以利用漏洞导致应用程序崩溃或控制受影响的系统。Apple 多个产品均出现了安全漏洞，远程攻击者可以利用漏洞窃取代码执行权限或者发起拒绝服务攻击。Linux Kernel 出现多个安全漏洞，本地攻击者可以利用漏洞获得敏感信息或者导致拒绝服务。另外，SAP 和 Google 的产品也出现安全漏洞，对互联网用户的信息安全和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、Nostromo nhttpd 发布升级程序修补多个安全漏洞

Nostromo nhttpd 是一款开源的 WEB 服务程序。本周，Nostromo nhttpd 发布了升级程序用于修复多个安全漏洞，以避免远程攻击者利用漏洞发起目录遍历或执行任意代码攻击。CNVD 已收录相关补丁，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/3301>
<http://www.cnvd.org.cn/patch/3302>



本周要闻速递

1. Adobe 披露 Flash/Reader/Acrobat 安全漏洞

Adobe 近日发布了一份安全公告 (APSA11-01)，指出 Adobe Flash Player、Adobe Reader 和 Acrobat 产品中都存在一个严重的安全问题 (CVE-2011-0609)。这个漏洞存在于以下平台版本：Windows、Mac、Linux 和 Solaris 平台最新 Adobe Flash Player 10.2.152.33 版本以及更早版本；Android 版 Flash Player 10.1.106.16 及更早版本；Windows 和 Mac 平台包含 authplay.dll 组件的 Adobe Reader/Acrobat X (10.0.1) 及更早版本。有人将嵌入 Flash (.swf) 文件的微软 Excel (.xls) 文档以附件形式发送，当用户打开该附件就会被攻击。目前，Adobe 尚未收到利用 Adobe Reader 和 Acrobat 的攻击报告。Adobe 表示，当前他们正在开发一个补丁并尽快为用户提供升级，预定于 3 月 21 日当周。由于 Adobe Reader X 中的保护模式可以保护用户免受此类型的攻击，因此 Adobe 计划在下一季度的例行安全补丁日再提供升级，具体日期为 6 月 14 日。

参考链接：<http://tech.163.com/digi/11/0315/15/6V6PN82A00162OUT.html>

2. 黑莓 OS 6 被发现 JavaScript 脚本漏洞

在今年的 Pwn2Own 黑客挑战赛中，黑莓 OS 6 不幸中标被黑客们发现一个 JavaScript 脚本漏洞，会威胁到安装有黑莓 OS 6 系统的手机用户。如果用户访问恶意网站，就存在黑客利用该漏洞通过浏览器访问设备上的用户数据的风险。目前 RIM 已经建议企业用户和普通用户关闭自己黑莓设备浏览器中的 JavaScript 功能。实际上，黑莓手机的这次漏洞风波并没有想象中的那样危险，虽然这个漏洞是在黑客竞赛中被发现的，但是目前还没有公开借助该漏洞盗取用户数据的事件发生。另外这个漏洞仅限于黑莓 OS 6 系统，可以读取手机内部存储或者存储卡中的媒体文件，而不是电子邮件、日历、联系人等隐私信息。目前在浏览器设置中禁用 JavaScript 功能可以彻底阻止该漏洞生效。

参考链接：<http://news.mydrivers.com/1/188/188791.htm>

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