

信息安全漏洞周报

2011 年 2 月 28 日-2011 年 3 月 6 日

2011 年第 9 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、整理信息安全漏洞 119 个，其中高危漏洞 50 个、中危漏洞 16 个、低危漏洞 53 个。上述漏洞中，可利用来实施远程攻击的漏洞有 108 个。网上已经出现针对“Microsoft Visual Studio 项目文件缓冲区溢出漏洞”、“Linux Kernel '/proc/'权限处理本地安全绕过漏洞”等零日漏洞的攻击代码，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 70 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 安全漏洞

Google Chrome 是一款流行的 WEB 浏览器。本周，Google Chrome 被披露存在多个综合评级为“高危”的漏洞。攻击者可以利用这些漏洞获得敏感信息或发起拒绝服务和执行任意代码攻击。CNVD 收录的漏洞包括：Google Chrome 布局处理存在悬浮指针漏洞、Google Chrome 'blocked'插件处理存在漏洞、Google Chrome 的 pickle 反序列化存在漏洞、Google Chrome 内部扩展函数泄露漏洞、Google Chrome 渲染 SVG 内容存在未明漏洞、Google Chrome 整数溢出漏洞、Google Chrome 的 WebGL 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 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-2011-04448>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04447>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04446>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04445>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04444>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04443>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04442>

2、Mozilla 产品安全漏洞

Mozilla Firefox/Thunderbird/SeaMonkey 是 Mozilla 发布的 WEB 浏览器/邮件客户端/网络套件。本周，Mozilla 发布公告披露 Firefox/Thunderbird/SeaMonkey 存在的多个安全漏洞。远程攻击者可以利用这些漏洞对应用程序发起拒绝服务、执行任意代码或提升权限等攻击。CNVD 收录的漏洞包括：Mozilla Firefox/Thunderbird/SeaMonkey 图像存储缓冲区溢出漏洞（CVE-2011-0061）、Mozilla Firefox/SeaMonkey 缓冲区溢出漏洞（CVE-2011-0058、CVE-2011-0054）、Mozilla Firefox/SeaMonkey 字符串映射漏洞（CVE-2011-0056）、Mozilla 中'JSON.stringify'函数释放后使用漏洞（CVE-2011-0055）、Mozilla Firefox/SeaMonkey 递归调用漏洞（CVE-2011-0051）及 Mozilla Firefox/SeaMonkey 未明安全漏洞（CVE-2011-0057）。上述漏洞的综合评级均为“高危”。目前厂商尚未发布这些漏洞的补丁程序，CNVD 建议用户随时关注厂商主页，以获取最新版本。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04422>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04420>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04419>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04418>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04417>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04416>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04415>

3、Apple WebKit 安全漏洞

Apple Safari 是一款基于 WebKit 引擎的 WEB 浏览器。本周，Apple Safari 的 WebKit 引擎出现了多个综合评级为“高危”的安全漏洞。CNVD 收录的漏洞包括：Apple Webkit 错误消息变化远程代码执行漏洞、Apple Safari Webkit Runin Box 提示远程代码执行漏洞、Apple Webkit Root HTMLBRElement 样式远程代码执行漏洞、Apple Webkit 字形布局远程代码执行漏洞、Apple Webkit setOuterText 内存破坏远程代码执行漏洞、Apple Safari Web Kit Range 对象远程代码执行漏洞。远程攻击者可以利用这些漏洞执行任意代码。目前，Apple 已经发布了补丁程序修复这些漏洞，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-2011-04479>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04478>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04477>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04476>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04475>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04473>

4、PDF-Pro 安全漏洞

PDF-Pro 是一款 PDF 文件制作与管理软件。本周，PDF-Pro 出现了多个综合评级为“高危”的安全漏洞。攻击者可以利用漏洞执行任意代码攻击或窃取敏感信息。CNVD 收录的

漏洞包括：PDF-Pro 上传任意文件漏洞、PDF-Pro 下载任意文件漏洞、PDF-Pro 删除任意文件漏洞、PDF-Pro 'ePapyrusReader.ocx'漏洞、PDF-Pro 内存释放漏洞、PDF-Pro 缓冲区溢出漏洞、PDF-Pro 装载库漏洞。目前厂商尚未发布这些漏洞的补丁程序，CNVD 建议用户及时关注厂商主页，以获取最新版本。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04469>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04468>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04467>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04466>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04465>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04464>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04463>

5、Microsoft Visual Studio 项目文件缓冲区溢出漏洞

Microsoft Visual Studio 是一款微软公司的开发工具套件系列产品。Microsoft Visual Studio 由于未能正确处理特制的项目文件，攻击者可以诱使用户打开经过精心构造的相同后缀名的文件，并在受影响的程序中执行任意代码。目前，互联网上已经出现针对该漏洞的攻击代码，主要影响版本为 Microsoft Visual Studio 9.0。厂商尚未发布此漏洞的补丁程序，CNVD 提醒广大用户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-2011-04396>

小结：本周，Mozilla 在官网上发布安全公告，公布了 Firefox/Thunderbird/SeaMonkey 多个产品的多个安全漏洞。远程攻击者可以利用这些漏洞对应用程序发起拒绝服务、执行任意代码或提升权限等攻击。Google Chrome 浏览器、Apple Safari 的 WebKit 引擎和 PDF-Pro 软件均出现了多个综合评级为“高危”的安全漏洞。微软的 Visual Studio 产品出现缓冲区溢出漏洞，网上已出现针对该漏洞的攻击代码，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、Moodle 发布升级程序修补了多个安全漏洞

Moodle 是一款开放源代码的网络教学应用程序。本周，Moodle 发布了升级程序用于修复多个安全漏洞，以避免攻击者利用漏洞绕过安全限制，获得敏感信息，进行跨站脚本等攻击。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/3151>
<http://www.cnvd.org.cn/patch/3152>
<http://www.cnvd.org.cn/patch/3153>
<http://www.cnvd.org.cn/patch/3155>



本周要闻速递

1. 谷歌修复 Gmail 存储软件更新漏洞

美国谷歌公司 3 月 1 日宣布，将修复“吉邮”（Gmail）存储软件更新漏洞，同时恢复用户遗失的邮件信息。一些“吉邮”用户 2 月底发现，收件箱信件“不翼而飞”。针对这一状况，谷歌技术副总裁在博客文章中说，“好消息是邮件从未丢失”，“为保护信息不受异常漏洞影响，我们把信息备份在存储器内”，但由于存储器处于离线状态，工作人员需耗费更长时间取回信息。现在，多数受影响账户已经恢复。谷歌说 0.02% 的“吉邮”用户受漏洞影响，但未公开用户总数。

参考链接：http://news.ccidnet.com/art/11099/20110302/2322213_1.html

2. 微软下周二将发布 3 月份补丁更新

3 月 4 日消息，据国外媒体报道，与上个月的“补丁星期二”修复多达 22 个安全漏洞不同，微软将在下周发布 3 个补丁仅修复 4 个安全漏洞。微软周四发布的安全公告通知称，微软下周二将发布 3 个安全补丁，其中一个修复 Windows 安全漏洞的“严重”等级的补丁，其它两个补丁是“重要”等级的，修复 Windows 和 Office 中的安全漏洞。这些安全漏洞都涉及到远程执行代码。这意味着攻击者能够在目标计算机上强制执行代码，从而完全控制那台计算机。

参考链接：http://news.ccidnet.com/art/1032/20110304/2324889_1.html

3. 谷歌修复浏览器漏洞，奖励漏洞报告者 1.4 万美元

3 月 2 日消息，据国外媒体报道，谷歌于本周一修复了 19 个 Chrome 浏览器漏洞，并向九位报告了这些漏洞的研究人员支付了共 1.4 万美元的奖励。本次谷歌将针对 Chrome 9.0.597 版本修复 16 个高危漏洞（“高危”级别也是谷歌危险系统中的第二严重的危险级别），此外还有 3 个中等漏洞。据了解，谷歌以及火狐浏览器的制造商 Mozilla 是目前提供奖励漏洞发现者的两家浏览器开发商。

参考链接：<http://cloud.csdn.net/a/20110302/292832.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