

信息安全漏洞周报

2011 年 8 月 15 日-2011 年 8 月 21 日

2011年第33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 101 个，其中高危漏洞 46 个、中危漏洞 52 个、低危漏洞 3 个。上述漏洞中，可利用来实施远程攻击的漏洞有 90 个。网上已经出现针对“FlexNet License Server Manager 远程代码执行漏洞”、“Notepad++下的 NppFTP 插件 LIST 命令远程堆缓冲区溢出漏洞”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。本周收录的漏洞中，已有 72 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。

成员单位报送漏洞统计

本周，共 5 家成员单位和 5 位个人报送了本周收录的全部 101 个漏洞，各单位报送情况如表 1 所示。其中，启明星辰、绿盟科技、恒安嘉新报送的数量较多。其中，国家互联网应急中心、北京邮电大学等单位的多位个人报送者报告了“深信服 SSLVPN 系统”存在的两个高危漏洞，目前已经纳入 CNVD 处置工作流程。

报送单位或个人	漏洞报送数量	私有漏洞数量
启明星辰	65	0
绿盟科技	57	0
恒安嘉新	36	0
安氏领信	3	0
安天	4	0
个人上报者	3	3
总计	101（去重）	3

表 1 成员单位上报漏洞统计表

本周，CNVD 整理和发布的漏洞涉及 Mozilla、WordPress、IBM、Apple、Microsoft 等多家厂商的产品，漏洞数量按厂商统计如表 2 所示。

序号	厂商（产品）	漏洞数量	所占比例
1	Mozilla	15	14.9%
2	WordPress	13	12.9%
3	Real Networks	11	10.9%
4	Ruby On Rails	5	5.0%
5	PHP	3	3.0%
6	IBM	2	2.0%
7	Linux	2	2.0%
8	EMC	2	2.0%
9	Apple	2	2.0%
10	Microsoft	2	2.0%
11	其它	44	43.3%

表 2 漏洞产品涉及厂商分类统计

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、Mozilla 产品安全漏洞

本周，Mozilla 发布安全更新，修补 Firefox 存在的多个安全漏洞。Mozilla Firefox 是 Mozilla 所发布的 WEB 浏览器/电子邮件客户端/新闻组客户端。攻击者可以利用漏洞获得敏感信息、绕过安全限制、操作数据或发起拒绝服务和特权提升攻击。CNVD 收录的相关漏洞包括：Mozilla Firefox appendchild 虚指针引用漏洞、Mozilla Firefox 跨源数据窃取漏洞、Mozilla Firefox 敏感信息泄露漏洞、Mozilla Firefox ANGLE 库堆溢出漏洞、Mozilla Firefox WebGL shaders 拒绝服务漏洞、Mozilla Firefox 未签名脚本安全绕过漏洞、Mozilla Firefox 内存破坏漏洞（CVE-2011-2985、CVE-2011-2992）等。除“Mozilla Firefox 跨源数据窃取漏洞、Mozilla Firefox 敏感信息泄露漏洞”外，其余漏洞的综合评级均为“高危”。CNVD 提醒广大 Mozilla 用户尽快下载补丁更新，避免引发漏洞相关的网络安全事件。

参考链接：
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06863>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06861>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06858>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06856>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06853>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06851>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06848>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06847>

2、Real Networks RealPlayer 安全漏洞

RealNetworks RealPlayer 是一款媒体播放程序。本周，Real Networks RealPlayer 被披露存在多个安全漏洞。攻击者利用漏洞构建恶意 WEB 页，诱使用户解析，以应用程序上下文执行任意代码。CNVD 收录的相关漏洞包括：Real Networks RealPlayer 内存破坏漏洞（CVE-2011-2954、CVE-2011-2952、CVE-2011-2955）、Real Networks RealPlayer 远程堆缓冲区溢出漏洞（CVE-2011-2945）、Real Networks RealPlayer ActiveX 控件越界远程代码执行漏洞（CVE-2011-2953）、Real Networks RealPlayer ActiveX 控件远程代码执行漏洞（CVE-2011-2946）、Real Networks RealPlayer 跨域脚本远程代码执行漏洞、Real Networks RealPlayer QCP 解析远程代码执行漏洞。上述漏洞的综合评级均为“高危”。目前，厂商已经发布上述漏洞的补丁程序，CNVD 提醒广大用户尽快下载补丁更新，避免引发漏洞相关的网络安全事件。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06869>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06867>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06864>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06865>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06860>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06836>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06831>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06830>

3、Linux 产品安全漏洞

Linux 是一款开源的操作系统。本周，Linux Kernel 出现多个本地安全漏洞。攻击者利用漏洞提升特权或进行拒绝服务攻击，使系统崩溃。CNVD 收录的相关漏洞包括：Linux Kernel 'perf_count_sw_cpu_clock'事件拒绝服务漏洞、Linux Kernel OOPS 'qdisc_dev()'拒绝服务漏洞、Linux Kernel 'perf'工具本地特权提升漏洞。目前，厂商已经发布上述漏洞的补丁程序，CNVD 提醒广大 Linux 用户尽快下载补丁更新，避免引发漏洞相关的网络安全事件。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06813>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06805>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06792>

4、WordPress 产品安全漏洞

本周，WordPress 被披露存在多个安全漏洞。攻击者可以利用漏洞发起 SQL 注入攻击、执行任意代码或获得敏感信息。CNVD 收录的相关漏洞包括：WordPress IP Logger

插件'map-details.php' SQL 注入漏洞、WordPress 存在未明远程漏洞（CVE-2011-3130、CVE-2011-3129、CVE-2011-3128、CVE-2011-3127、CVE-2011-3126、CVE-2011-3122）、WordPress OdiHost Newsletter 插件 SQL 注入漏洞等。上述漏洞中“WordPress IP Logger 插件'map-details.php' SQL 注入漏洞”、“WordPress 存在未明远程漏洞(CVE-2011-3130、CVE-2011-3129、CVE-2011-3122)”的综合评级为“高危”。CNVD 提醒广大 WordPress 用户尽快下载补丁更新，避免引发漏洞相关的网络安全事件。

参考链接: <http://www.cnvd.org.cn/vulnerability/CNVD-2011-06833>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06825>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06824>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06823>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06821>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06819>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06817>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06870>

5、FlexNet License Server Manager 远程代码执行漏洞

FlexNet License Server Manager 是一款许可证服务管理程序。默认监听 TCP 27000 端口的证书服务管理器存在缺陷，由于目录遍历问题和一些文件重命名缺陷，攻击者可以利用这些漏洞以证书服务器管理守护程序上下文执行任意代码。目前，厂商尚未发布该漏洞的修补程序，CNVD 提醒广大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-2011-06839>

小结：本周，Mozilla 发布安全更新，修补 Firefox 多个产品存在的多个安全漏洞。攻击者可以利用漏洞获得敏感信息，绕过安全限制，操作数据，或进行拒绝服务和特权提升攻击，对使用 Mozilla 产品的用户构成较为严重的威胁。同时，Real Networks、Linux 和 WordPress 产品也被披露存在多个安全漏洞。此外，FlexNet License Server Manager 零日漏洞也对使用该产品的用户构成较大威胁。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、Ruby on Rails 发布升级程序，修补多个安全漏洞

Ruby on Rails 是一款 Web 应用程序框架，构建在 Ruby 语言之上。本周，Ruby on Rails 发布升级程序，修复了多个安全漏洞。攻击者可以利用漏洞执行任意代码。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/4798>

<http://www.cnvd.org.cn/patch/4797>

<http://www.cnvd.org.cn/patch/4802>

<http://www.cnvd.org.cn/patch/4801>

<http://www.cnvd.org.cn/patch/4800>



本周要闻速递

1. 工业系统漏洞被黑客广泛利用

拉斯韦加斯举行的“黑帽”和 Defcon 两场黑客大会上公布的最惊人的一些研究, 揭示了发电站、化工厂、配水系统和全世界其他工业设施所使用的老旧电脑系统中存在的弱点。专业研究公司发现了德国西门子公司工业控制系统中的一个“后门”, 它可以让黑客摧毁核电站、油气管道、水处理系统、制药厂以及其他关键设施。去年夏天, 研究人员发现了“震网”(Stuxnet 病毒), 这是一种用于攻击西门子工业控制系统的计算机蠕虫病毒。“震网”曾被用于攻击伊朗的核浓缩设施, 以打击该国的核项目。一些专家将“震网”描述为针对伊朗核项目的“制导网络导弹”。美国国土安全部上月警告国会说, 黑客们很可能正在修改“震网”的代码, 制造能够对世界任何地方的工业控制系统发动进攻的新武器。“震网”方面的专家说, 这些系统中的许多密码都是通过硬编码固化在设备中的, 这意味着无法修改它们。这使得它们很容易成为攻击对象。

参考链接: <http://www.2cto.com/News/201108/101015.html>

2. 每部 PC 存在 12 个安全漏洞

来自专业安全厂商的研究显示, 平均每部 PC 都存在 12 种不同的安全漏洞。截止今年第二季度, 研究人员在实验对象的系统中检测到 27289171 个包含漏洞的应用程序和文件, 漏洞涉及的相关部件主要是 Adobe 旗下的 Reader、Flash、Shockwave 和 JavaJDK 等。安全公司认为, 伴随 Window 自动更新机制和较高的 Win7 使用率, PC 的安全性能越来越好。但某些应用程序成为系统的大漏洞, 仅 AdobeFlash 就出现多个高危漏洞。

参考链接: <http://roll.sohu.com/20110819/n316758714.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