

## 信息安全漏洞周报

2011 年 9 月 19 日-2011 年 9 月 25 日

2011 年 第38 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**高**。

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 135 个，其中高危漏洞 63 个、中危漏洞 69 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 128 个。网上已经出现针对“IBM Lotus Domino 'NSFComputeEvaluateExt()'函数远程栈缓冲区溢出漏洞”、“Apple Mac OS X Lion Directory Services 安全绕过漏洞”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 71 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 家成员单位和北京邮电大学的安全专家报送了本周收录的全部 135 个漏洞，各单位报送情况如表 1 所示。其中，绿盟科技、启明星辰、恒安嘉新的数量较多。

| 报送单位或个人 | 漏洞报送数量  | 私有漏洞数量 |
|---------|---------|--------|
| 绿盟科技    | 87      | 0      |
| 启明星辰    | 72      | 0      |
| 恒安嘉新    | 59      | 0      |
| 安天      | 33      | 0      |
| 安氏领信    | 5       | 0      |
| 北京邮电大学  | 2       | 2      |
| 总计      | 135（去重） | 2      |

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 Google、WordPress、Adobe、Red Hat、netvisions 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  | Google      | 33   | 24.4% |
| 2  | WordPress   | 17   | 12.6% |
| 3  | Adobe       | 5    | 3.7%  |
| 4  | Red Hat     | 5    | 3.7%  |
| 5  | net4visions | 4    | 3%    |
| 6  | Cisco       | 3    | 2.2%  |
| 7  | FFmpeg      | 3    | 2.2%  |
| 8  | IBM         | 3    | 2.2%  |
| 9  | Linux       | 3    | 2.2%  |
| 10 | SAP         | 2    | 1.5%  |
| 11 | 其它          | 57   | 42.3% |

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、pNetPower 6.1 AngelServer UDP 数据包堆缓冲区溢出漏洞补丁衍生拒绝服务漏洞

本周，CNVD 发布了关于“pNetPower 6.1 AngelServer UDP 数据包堆缓冲区溢出漏洞”补丁的一个衍生拒绝服务漏洞。CNVD 于 2011 年 5 月 20 日发布了北京三维力控科技有限公司（简称三维力控公司）生产的 pNetPower 电力版监控组态软件存在的缓冲区溢出漏洞。三维力控公司随后推出了该漏洞的补丁包。9 月 2 日，CNVD 接到成员单位北京神州绿盟科技有限公司分析上报，称该补丁包由于对关键参数未进行 SEH 保护，从而引入了新的拒绝服务漏洞。CNVD 对该新衍生漏洞进行了测试验证，并于 9 月 23 日正式发布漏洞公告。漏洞详情请参考 CNVD 官网相关信息。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07098>

### 2、Google Chrome 安全漏洞

本周，Google 发布安全更新，修复了 Chrome 浏览器存在的多个漏洞。远程攻击者可以利用漏洞绕过部分安全限制、获得敏感信息、执行任意代码或使应用程序崩溃。CNVD 收录的相关漏洞包括：Google Chrome 类型混淆漏洞（CVE-2011-2875）、Google Chrome 越界读漏洞（CVE-2011-2858）、Google Chrome 存在未明漏洞（CVE-2011-2862）、Google Chrome 读取破坏漏洞（CVE-2011-2861）、Google Chrome 内存错误引用漏洞（CVE-2011-2860）、Google Chrome 自签名证书漏洞（CVE-2011-2874）。除“Google Chrome 读取破坏漏洞（CVE-2011-2861）”和“Google Chrome 越界读漏洞（CVE-2011-2858）”

的综合评级为“中危”外，其他均为“高危”。CNVD 提醒 Google 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-2011-07430>  
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07429>  
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07427>  
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07425>  
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07424>  
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07421>

### 3、Adobe Flash Player 安全漏洞

Adobe Flash Player 是一款 Flash 文件处理程序。本周，Adobe Flash Player 被披露存在多个安全漏洞。攻击者可以利用漏洞以应用程序上下文执行任意代码或窃取敏感信息。CNVD 收录的漏洞包括：Adobe Flash Player 安全限制绕过信息泄露漏洞、Adobe Flash Player 逻辑错误远程代码执行漏洞、Adobe Flash Player AVM 栈溢出漏洞（CVE-2011-2426）、Adobe Flash Player AVM 栈溢出漏洞（CVE-2011-2427）、Adobe Flash Player 流媒体逻辑错误远程代码执行漏洞、Adobe Flash Player 存在未明漏洞。上述漏洞中，除“Adobe Flash Player 安全限制绕过信息泄露漏洞、Adobe Flash Player 存在未明漏洞”的综合评级为“中危”外，其他均为“高危”。目前，Adobe 已经发布了这些漏洞的补丁程序，CNVD 提醒相关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-2011-07446>  
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07445>  
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07437>  
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07436>  
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07435>  
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07381>

### 4、WordPress 插件安全漏洞

本周，WordPress 多款插件被披露存在多个漏洞。攻击者可以利用该产品漏洞获得敏感信息、执行任意代码或控制应用程序。CNVD 收录的相关漏洞包括：Wordpress Relocate 上传插件远程文件包含漏洞、WordPress 插件 Count Per Day 'month' SQL 注入漏洞、WordPress 插件 Filedownload 'path'文件泄露漏洞、WordPress 插件 WP Forum SQL 注入漏洞、WordPress 插件 WP DS FAQ SQL 注入漏洞、WordPress 插件 Disclosure Policy 'abspath'远程文件包含漏洞。其中，“WordPress 插件 Count Per Day 'month' SQL 注入漏洞、WordPress 插件 WP Forum SQL 注入漏洞、WordPress 插件 WP DS FAQ SQL 注入漏洞”的综合评级为“高危”，且部分漏洞的攻击代码已在互联网出现。目前，厂商尚未发布上述漏洞的补丁程序，CNVD 提醒相关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-2011-07449>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07374>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07367>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07366>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07362>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07359>

## 5、Cisco 产品安全漏洞

本周，Cisco 的产品 TelePresence 和 Identity Services Engine 存在多个安全漏洞。攻击者可以利用漏洞获得管理员权限、执行脚本代码或发起拒绝服务攻击。CNVD 收录的相关漏洞包括：Cisco TelePresence Endpoint 内存破坏漏洞、Cisco TelePresence Endpoint HTML 注入漏洞、Cisco Identity Services Engine 数据库默认验证凭据安全绕过漏洞。其中，“Cisco TelePresence Endpoint 内存破坏漏洞、Cisco Identity Services Engine 数据库默认验证凭据安全绕过漏洞”的综合评级为“高危”。目前，Cisco 已经发布上述漏洞的修补程序，CNVD 提醒相关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-2011-07400>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07399>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07383>

## 6、IBM Lotus Domino 'NSFComputeEvaluateExt()'函数远程栈缓冲区溢出漏洞

Lotus Domino 是 IBM 生产的基于 WEB 的办公协作平台软件。本周，IBM Lotus Domino 被披露存在一个栈缓冲区溢出漏洞。由于 WebAdmin.nsf 模块未能正确地进行边界检查，远程验证攻击者可以通过发送特制的 HTTP POST 请求，造成缓冲区溢出，进而以 SYSTEM 特权执行任意代码或导致应用程序拒绝服务。目前，互联网上已经出现针对该漏洞的攻击代码，主要影响 IBM Lotus Domino 8.5.2 版本。厂商尚未发布该漏洞的补丁程序，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-2011-07384>

小结：本周，Google 发布安全更新，修复了 Chrome 浏览器存在的多个漏洞。攻击者可以利用这些漏洞远程攻击者可以利用漏洞绕过部分安全限制，获得敏感信息，执行任意代码或使应用程序崩溃。Adobe Flash Player、Cisco 产品和 Wordpress 插件也被披露存在多个漏洞。此外，IBM Lotus Domino 零日漏洞也对使用该产品的用户造成较严重威胁，有可能引发针对相关目标的网络攻击事件。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、Linux 发布升级程序，修补 Kernel 安全漏洞

本周，Linux 发布升级程序，修补了 Kernel 存在的多个安全漏洞。攻击者可以利用漏洞进行拒绝服务攻击。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/5176>

<http://www.cnvd.org.cn/patch/5168>

## 本周要闻速递

### 1. Oracle 发现 HTTP 服务器产品安全漏洞

9 月 21 日消息，据国外媒体报道，日前 Oracle 公司建议管理员对系统进行更新，原因是在该公司基于 Apache 2.0 或 2.2 的 HTTP 服务器产品中发现了重大的安全漏洞。漏洞组件存在于 Fusion Middleware 11g 和 Application Server 10g 平台中，会引发拒绝服务攻击。该漏洞可以被远程利用，无需本地登录或者用户名密码等合法认证。Oracle 的这次更新紧跟微软公司的最新补丁更新，这次更新包括五个安全修复以及一个用来去除若干 DigitNotar 证书的更新。若干天前，DigitNotar 证书被证实可以被黑客利用。

参考链接：[http://news.ccidnet.com/art/945/20110921/2794179\\_1.html](http://news.ccidnet.com/art/945/20110921/2794179_1.html)

### 2. 漏洞网站称 ATM 取款机存在安全漏洞

9 月 21 日，国内某漏洞网站爆出新闻，指网上爆出 ATM 取款机存在漏洞，黑客可获最高权限，通过入侵 ATM 机可窃取银行卡帐号密码、进行转账等操作。安全专家提醒说，从技术角度讲 ATM 取款机的漏洞确实存在，尤其是那些带有全键盘输入或虚拟键盘输入的“高级取款机”，更容易被黑客入侵。临近国庆取钞高峰，广大银行卡用户应注意安全。

参考链接：<http://sec.chinabyte.com/15/12166515.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](http://www.cert.org.cn)

邮箱：[vreport@cert.org.cn](mailto:vreport@cert.org.cn)

电话：010-82990999