

## 信息安全漏洞周报

2012 年 7 月 2 日-2012 年 7 月 8 日

2012 年第 27 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 118 个，其中高危漏洞 37 个、中危漏洞 70 个、低危漏洞 11 个。上述漏洞中，可利用来实施远程攻击的漏洞有 109 个。本周收录的漏洞中，已有 69 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。本周互联网上出现“Solar FTP Server 拒绝服务漏洞”、“ComSndFTP 服务器格式字符串漏洞”等的零日攻击代码，请使用相关产品的用户注意加强防范。

### 成员单位报送漏洞统计

本周，共 7 家成员单位和多个合作伙伴报送了本周收录的全部 118 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、天融信、安天实验室等单位报送数量较多。此外，上海交通大学、信息安全共性技术国家工程研究中心以及个人漏洞研究者向 CNVD 提交了 4 个原创漏洞。

| 报送单位或个人 | 漏洞报送数量 | 原创漏洞数量 |
|---------|--------|--------|
| 启明星辰    | 64     | 0      |
| 绿盟科技    | 37     | 0      |
| 安天实验室   | 29     | 0      |
| 恒安嘉新    | 23     | 0      |
| 天融信     | 20     | 0      |
| 安氏领信    | 7      | 0      |
| 东软      | 4      | 0      |
| 上海交通大学  | 2      | 2      |
| 个人报送者   | 1      | 1      |

|                  |         |   |
|------------------|---------|---|
| 信息安全共性技术国家工程研究中心 | 1       | 1 |
| 报送总计             | 188     | 4 |
| 录入总计             | 118（去重） | 4 |

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Wordpress、Drupal、Pro-face、Microsoft、WellinTech 等多家厂商的产品，部分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  | Wordpress  | 9    | 8%   |
| 2  | Drupal     | 6    | 5%   |
| 3  | Pro-face   | 5    | 4%   |
| 4  | Microsoft  | 5    | 4%   |
| 5  | WellinTech | 5    | 4%   |
| 6  | Winamp     | 4    | 3%   |
| 7  | Linux      | 3    | 2%   |
| 8  | Nagios     | 3    | 2%   |
| 9  | Revelation | 3    | 2%   |
| 10 | Apple      | 1    | 1%   |
| 11 | 其它         | 74   | 65%  |

表 2 漏洞产品涉及厂商分布统计表

漏洞按影响类型统计

本周，CNVD 收录了 118 个漏洞。其中操作系统漏洞 5 个，应用程序漏洞 67 个，WEB 应用漏洞 41 个，网络设备漏洞 2 个，安全产品漏洞 3 个。

| 漏洞影响对象类型 | 漏洞数量 |
|----------|------|
| 操作系统漏洞   | 5    |
| 应用程序漏洞   | 67   |
| WEB 应用漏洞 | 41   |
| 网络设备漏洞   | 2    |
| 数据库漏洞    | 0    |
| 安全产品漏洞   | 3    |

表 3 漏洞按影响类型统计表

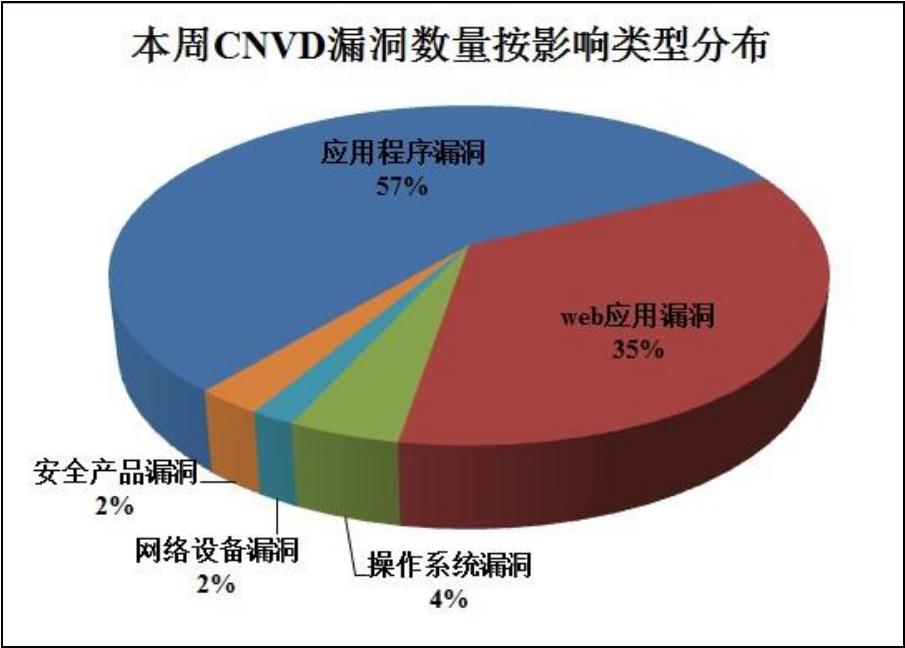


图 1 本周漏洞按影响类型分布

### 本周涉及电信行业漏洞信息

本周，CNVD 收录了 2 个网络设备漏洞。其中，“Huawei HG866 'password.html'安全限制绕过漏洞”的综合评级为“高危”，“Edimax IC-3030iWn UDP 报文密码信息泄露漏洞”的综合评级均为“中危”。目前，互联网上已经出现了针对“Edimax IC-3030iWn UDP 报文密码信息泄露漏洞”的攻击代码。

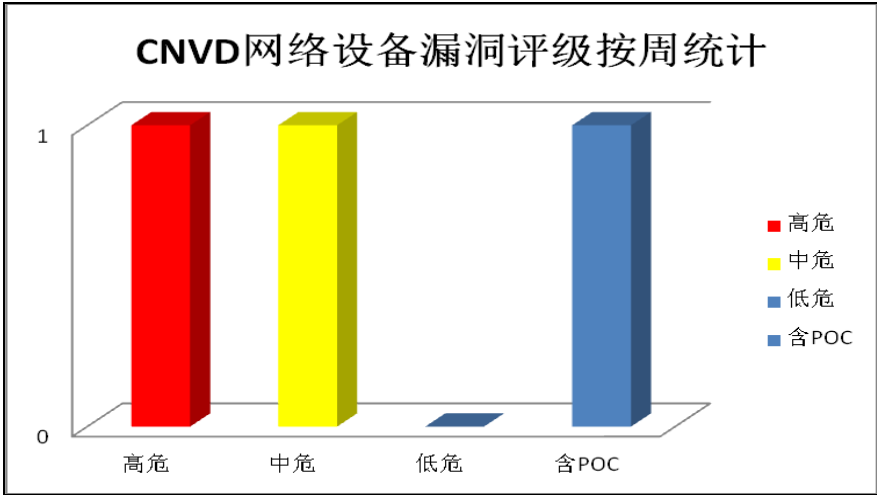


图 2 网络设备漏洞统计

### 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、Microsoft 产品安全漏洞

Microsoft IIS 是一款微软开发的 WEB 应用服务程序。本周，该程序被披露存在多个安全漏洞，攻击者可利用漏洞非法访问受密码保护的资源并查看服务器进程内的源代码，获取敏感信息，发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Microsoft IIS 存在多个 FTP 命令请求拒绝服务漏洞、Microsoft IIS 文件枚举漏洞、Microsoft IIS 身份验证绕过漏洞、Microsoft IIS 源代码泄露漏洞、Microsoft IIS 短文件或文件夹名使用波浪号泄漏漏洞。目前，厂商尚未发布上述漏洞的修补程序。CNVD 提醒相关用户关注厂商主页及时更新，避免引发漏洞相关的网络安全事件。

参考链接：[http://www.cnvd.org.cn/sites/main/preview/ldgg\\_preview.htm?tid=51234](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=51234)  
[http://www.cnvd.org.cn/sites/main/preview/ldgg\\_preview.htm?tid=51197](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=51197)  
[http://www.cnvd.org.cn/sites/main/preview/ldgg\\_preview.htm?tid=51191](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=51191)  
[http://www.cnvd.org.cn/sites/main/preview/ldgg\\_preview.htm?tid=51192](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=51192)  
[http://www.cnvd.org.cn/sites/main/preview/ldgg\\_preview.htm?tid=51258](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=51258)

## 2、Winamp 安全漏洞

Winamp 是一款通用音乐播放器。本周，该产品被披露存在多个安全漏洞，攻击者可利用漏洞破坏内存，导致缓冲区溢出。

CNVD 收录的相关漏洞包括：Winamp AVI/IT 文件内存破坏漏洞（CNVD-2012-12786）、Winamp AVI/IT 文件堆缓冲区溢出漏洞（CNVD-2012-12785）、Winamp AVI/IT 文件堆缓冲区溢出漏洞（CNVD-2012-12784）、Winamp AVI/IT 文件堆缓冲区溢出漏洞（CNVD-2012-12783）。上述漏洞的综合评级均为“高危”。目前，厂商已经修复了上述漏洞。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/sites/main/preview/ldgg\\_preview.htm?tid=51165](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=51165)  
[http://www.cnvd.org.cn/sites/main/preview/ldgg\\_preview.htm?tid=51164](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=51164)  
[http://www.cnvd.org.cn/sites/main/preview/ldgg\\_preview.htm?tid=51163](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=51163)  
[http://www.cnvd.org.cn/sites/main/preview/ldgg\\_preview.htm?tid=51162](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=51162)

## 3、IBM 产品安全漏洞

IBM AIX 是一款商业主机操作系统；IBM Sterling B2B Integration 是一款应用于 B2B 业务模式的文档交互解决方案；IBM InfoSphere Guardium 是一款企业数据中心安全保障解决方案。本周，上述产品被披露存在多个安全漏洞，攻击者可利用上述漏洞造成受影响的计算机崩溃，发起拒绝服务攻击或提升特权。

CNVD 收录的相关漏洞包括：IBM Sterling B2B Integrator 存在多个漏洞、IBM AIX 临时文件创建漏洞、IBM InfoSphere Guardium 本地拒绝服务漏洞。厂商已经修复了上述漏洞。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/sites/main/preview/ldgg\\_preview.htm?tid=51232](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=51232)

[http://www.cnvd.org.cn/sites/main/preview/ldgg\\_preview.htm?tid=51183](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=51183)

[http://www.cnvd.org.cn/sites/main/preview/ldgg\\_preview.htm?tid=51180](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=51180)

#### 4、Drupal 模块安全漏洞

Drupal 是一款开放源码的内容管理平台。本周，Drupal 多个模块被披露存在多个漏洞。攻击者利用漏洞可劫持用户会话，利用脚本注入绕过白名单，发起钓鱼攻击。

CNVD 收录的相关漏洞包括：Drupal Authoring HTML 白名单安全旁路漏洞、Drupal Node Hierarchy 模块跨站请求伪造漏洞、Drupal Janrain Capture 模块重定向漏洞、Drupal filedepot 模块会话劫持漏洞、Drupal Protest 模块'protest\_body'跨站脚本漏洞、Drupal SimpleMeta 模块跨站请求伪造漏洞。厂商已经修复了上述漏洞。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/sites/main/preview/ldgg\\_preview.htm?tid=51214](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=51214)

[http://www.cnvd.org.cn/sites/main/preview/ldgg\\_preview.htm?tid=51209](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=51209)

[http://www.cnvd.org.cn/sites/main/preview/ldgg\\_preview.htm?tid=51210](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=51210)

[http://www.cnvd.org.cn/sites/main/preview/ldgg\\_preview.htm?tid=51211](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=51211)

[http://www.cnvd.org.cn/sites/main/preview/ldgg\\_preview.htm?tid=51213](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=51213)

[http://www.cnvd.org.cn/sites/main/preview/ldgg\\_preview.htm?tid=51212](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=51212)

#### 5、Solar FTP Server 拒绝服务漏洞

Solar FTP Server 是一款 FTP 服务程序。本周，Solar FTP Server 被披露存在一个拒绝服务漏洞。向 Solar FTP Server 发送多个并行处理的请求，可导致服务程序崩溃，造成拒绝服务攻击。目前，互联网上已经出现了针对该漏洞的攻击代码，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/sites/main/preview/ldgg\\_preview.htm?tid=51298](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=51298)

更多高危漏洞如表 3 所示，详细信息可根据 CNVD 编号，在 CNVD 官网进行查询。

参考链接：<http://www.cnvd.org.cn/publish/main/52/index.html>

| CNVD 编号         | 漏洞名称                  | 综合评级 | 修复方式                                                                                                                                                            |
|-----------------|-----------------------|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CNVD-2012-12834 | LIOOSYS CMS SQL 注入漏洞  | 高    | 暂无                                                                                                                                                              |
| CNVD-2012-12815 | Nagios XI SQL 盲注漏洞    | 高    | 用户可参考如下供应商提供的安全公告获得补丁信息：<br><a href="http://labs.nagios.com/2012/04/13/nagios-xi-ccm-full-beta/">http://labs.nagios.com/2012/04/13/nagios-xi-ccm-full-beta/</a> |
| CNVD-2012-12843 | MyClientBase SQL 注入漏洞 | 高    | 暂无                                                                                                                                                              |

|                 |                                                |   |                                                                                                                                                                                                                                                       |
|-----------------|------------------------------------------------|---|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CNVD-2012-12792 | ACDsee Pro 图形解析内存破坏漏洞（CNVD-2012-12792）         | 高 | 厂商已经发布了升级补丁以修复这个问题，请到厂商的主页下载：<br><a href="http://www.acdsystems.com/">http://www.acdsystems.com/</a>                                                                                                                                                  |
| CNVD-2012-12841 | KMPlayer DLL 加载漏洞                              | 高 | 暂无                                                                                                                                                                                                                                                    |
| CNVD-2012-12809 | Apple iTunes '.m3u'文件远程栈缓冲区溢出漏洞                | 高 | 厂商已经发布了升级补丁以修复这个问题，请到厂商的主页下载：<br><a href="http://support.apple.com/">http://support.apple.com/</a>                                                                                                                                                    |
| CNVD-2012-12780 | Huawei HG866 'password.html'安全限制绕过漏洞           | 高 | 暂无                                                                                                                                                                                                                                                    |
| CNVD-2012-12797 | IrfanView Formats PlugIn 'jpeg_ls.dll'堆缓冲区溢出漏洞 | 高 | IrfanView Formats PlugIn 4.34 已经修复此漏洞，建议用户下载使用：<br><a href="http://www.irfanview.com/plugins.htm">http://www.irfanview.com/plugins.htm</a><br><a href="http://www.irfanview.net/plugins/jpeg_ls.zip">http://www.irfanview.net/plugins/jpeg_ls.zip</a> |
| CNVD-2012-12794 | MyBB 'announcements.php'远程SQL注入漏洞              | 高 | 暂无                                                                                                                                                                                                                                                    |
| CNVD-2012-12790 | XnView 图形解压内存破坏漏洞（CNVD-2012-12790）             | 高 | 厂商已经发布了升级补丁以修复这个问题，请到厂商的主页下载：<br><a href="http://www.xnview.com/">http://www.xnview.com/</a>                                                                                                                                                          |

表 3 部分高危漏洞列表

小结：本周，Microsoft 和 IBM 的多款产品被披露存在多个漏洞，攻击者利用漏洞可获取敏感信息，造成受影响计算机崩溃，发起拒绝服务攻击。多个 Drupal 模块也被披露存在多个漏洞，攻击者利用漏洞可劫持用户会话，利用脚本注入绕过白名单，发起钓鱼攻击。利用 Winamp 存在的漏洞可破坏内存，导致缓冲区溢出，可利用发起针对桌面操作系统用户的攻击。此外，Solar FTP Server 服务器被披露存在零日漏洞，对网络服务器安全构成威胁，相关管理员用户需加强防范。

## 本周重要漏洞修补信息

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

Linux Kernel 是开源操作系统 Linux 所使用的内核。本周，Linux 发布升级程序，修补了 Kernel 存在的漏洞。本地攻击者利用漏洞可发起拒绝服务攻击。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/sites/main/preview/bdgg\\_preview.htm?tid=18553](http://www.cnvd.org.cn/sites/main/preview/bdgg_preview.htm?tid=18553)

[http://www.cnvd.org.cn/sites/main/preview/bdgg\\_preview.htm?tid=18552](http://www.cnvd.org.cn/sites/main/preview/bdgg_preview.htm?tid=18552)

[http://www.cnvd.org.cn/sites/main/preview/bdgg\\_preview.htm?tid=18551](http://www.cnvd.org.cn/sites/main/preview/bdgg_preview.htm?tid=18551)

## 本周要闻速递

### 1. 微软将发布 7 月安全更新修复 IE 9 漏洞

据国外媒体报道，微软将于 7 月 10 日，发布 9 个安全补丁。其中，3 个漏洞为“高危”级别，其余 6 项为“重要”。微软透露，3 个标记为“高危”的漏洞中，有一个是 IE 9 浏览器中的安全漏洞。该漏洞仅存在于 IE 9 浏览器，对旧版浏览器则毫无影响。除此之外，这 9 个补丁还将修复 Windows XP Service Pack 3 至 Windows Server 2008 中安全问题。

参考链接：<http://www.newhua.com/2012/0706/167178.shtml>

### 2. Tango 系统再曝漏洞 使用 IE 浏览器易死机

据悉，在浏览德国最流行的网站 Bild.de 时，Windows Phone 手机会经常出现死机的情况。并且指出出现宕机的设备绝大部分为 Windows Phone Tango，甚至是最新的 8773 版本，而 Windows Phone Mango 版本则并未出现问题。问题出在 IE 浏览器对大型页面进行渲染时导致内存不足，解决该问题的最好方式则是在 IE 浏览器的设置选项菜单中将网页显示模式首选项修改成手机网站模式。如果用户在使用过程确实出现死机，非诺基亚 800 和诺基亚 900 用户如果找不到软关机的方式，就只能通过拆卸电池进行强制重启。

参考链接：<http://mobile.163.com/12/0708/13/85T5GI2J0011665S.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](http://www.cert.org.cn)

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

电话: 010-82990999