

信息安全漏洞周报

2012 年 6 月 4 日-2012 年 6 月 10 日

2012 年第 23 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 106 个，其中高危漏洞 34 个、中危漏洞 66 个、低危漏洞 6 个。上述漏洞中，可利用来实施远程攻击的漏洞有 104 个。本周收录的漏洞中，已有 64 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“SN News 'visualiza.php' SQL 注入漏洞”、“Audio Editor Master '.cda' 文件处理远程缓冲区溢出漏洞”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 106 个漏洞。各单位报送情况如表 1 所示。其中，天融信、恒安嘉新、启明星辰、安天实验室等单位报送数量较多。此外，恒安嘉新、知道创宇、奇虎 360、上海交通大学以及一位个人漏洞研究者向 CNVD 提交了 12 个原创漏洞。

报送单位或个人	漏洞报送数量	原创漏洞数量
天融信	28	0
启明星辰	63	0
恒安嘉新	39	3
安天实验室	35	0
知道创宇	1	1
安氏领信	4	0
东软	3	0
奇虎 360	2	2
上海交通大学	5	5

个人报送者	1	1
报送总计	181	12
总计	106（去重）	12

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Mozilla、IBM、Wordpress、Drupal、Piwik 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	Mozilla	12	11.3%
2	IBM	11	10.4%
3	Wordpress	11	10.4%
4	Drupal	9	8.5%
5	Piwik	5	4.7%
6	Microsoft	3	2.8%
7	Membris	3	2.8%
8	zoph	3	2.8%
9	Ubuntu	2	1.9%
10	WebKit	1	0.9%
11	其它	46	43.5%

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 106 个漏洞。其中操作系统漏洞 3 个，应用程序漏洞 43 个，WEB 应用漏洞 52 个，网络设备漏洞 2 个，数据库漏洞 6 个。

漏洞影响对象类型	漏洞数量
操作系统漏洞	3
应用程序漏洞	43
WEB 应用漏洞	52
网络设备漏洞	2
数据库漏洞	6
安全产品漏洞	0

表 3 漏洞按影响类型统计表

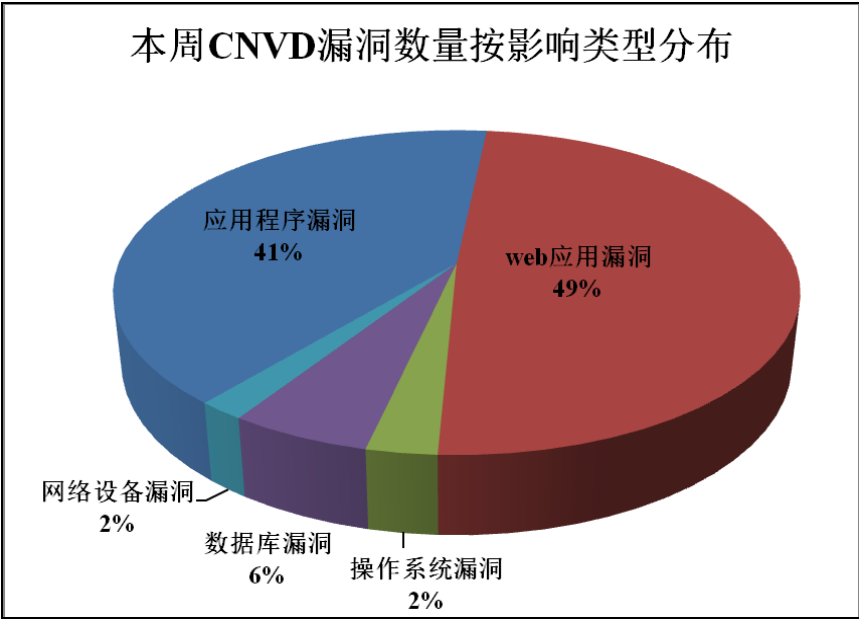


图 1 本周漏洞按影响类型分布

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，“ZTE Score M 手机硬编码漏洞”的综合评级为“高危”，“SEIL Routers HTTP-Proxy/Gateway 功能安全绕过漏洞”的综合评级均为“中危”。

此外，本周 ISC 官方披露的“ISC BIND DNS 资源记录处理远程拒绝服务漏洞”（CNVD-2012-12347）对电信行业影响较为广泛，涉及运营商和域名机构。根据评估，目前该漏洞对基础电信运营企业的递归服务器构成较为直接的威胁。

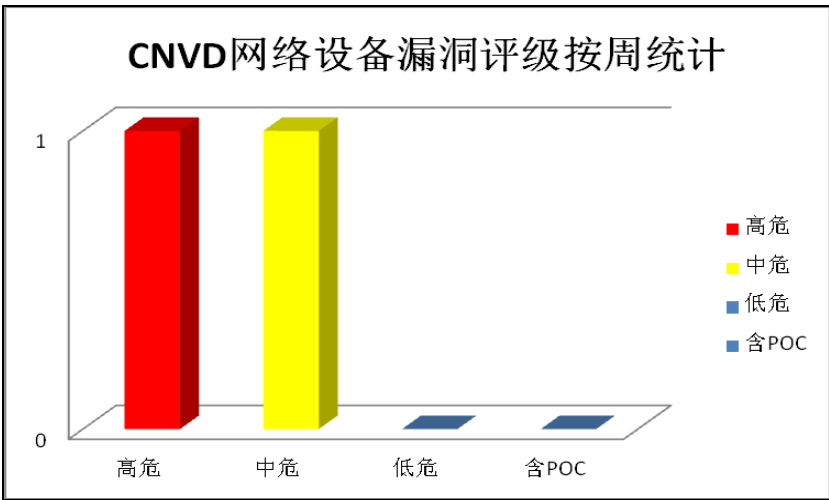


图 2 网络设备漏洞统计

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、ISC BIND 9 远程拒绝服务零日漏洞

6月4日，ISC 在其官网上公布了一个 ISC BIND 存在的远程拒绝服务零日漏洞。ISC BIND 是一款应用广泛的域名解析系统软件。BIND 允许将试验性资源记录的 RDATA 部分设置为空，然而当处理这些记录时，会诱发一些导致服务异常的情况。根据 ISC 发布的公告称，DNS 递归服务器可能会因此崩溃，或者将部分内存数据泄露给解析器；DNS 权威辅服务器有可能会在区传送完毕进行重启时发生崩溃；而 DNS 权威主服务器的区选项“auto-dnssec”若设置为“maintain”，则有可能导致权威主服务器区数据损坏。

CNVD 对该漏洞的综合评级为“高危”。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，同时可升级到 BIND 9.6-ESV-R7-P1, 9.7.6-P1, 9.8.3-P1, 9.9.1-P1 版本，以减轻该漏洞威胁。

参考链接：http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=50156

2、Mozilla 产品安全漏洞

Mozilla Firefox/SeaMonkey/Thunderbird 是 Mozilla 所发布的 WEB 浏览器/新闻组客户端/邮件客户端。本周，上述 Mozilla 产品被披露存在多个漏洞。攻击者可以利用漏洞构建恶意链接，诱使用户解析，使应用程序崩溃或执行任意代码。

CNVD 收录的相关漏洞包括：Mozilla Firefox/SeaMonkey/Thunderbird 内存错误引用漏洞、Mozilla Firefox/SeaMonkey/Thunderbird 堆缓冲区溢出漏洞(CNVD-2012-12367、CNVD-2012-12369)、Mozilla Firefox/Thunderbird/SeaMonkey 内存破坏漏洞(CNVD-2012-12381、CNVD-2012-12384、CNVD-2012-12382)、Mozilla Firefox/Thunderbird/SeaMonkey 内存错误引用远程代码执行漏洞、Mozilla Firefox/SeaMonkey/Thunderbird 本地特权提升漏洞（CNVD-2012-12375）等。上述漏洞的综合评级均为“高危”，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=50215
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=50216
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=50218
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=50257
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=50261
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=50260
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=50258
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=50238

3、IBM 产品安全漏洞

IBM DB2 是一款关系型数据库管理系统；IBM WebSphere Sensor Events 是一个针对

传感器解决方案而设计开发的中间件产品平台；IBM WebSphere Application Server (WAS) 是 IBM 开发的一款应用服务器。本周，上述产品被披露存在多个安全漏洞，攻击者利用漏洞可以获得敏感信息、提升特权、发起跨站或拒绝服务攻击。

CNVD 收录的相关漏洞包括：IBM WebSphere Sensor Events 'searchView.jsp'跨站脚本漏洞、IBM WebSphere Sensor Events 'deferredView.jsp'跨站脚本漏洞、IBM WebSphere Sensor Events HTTP methods 存在未明漏洞、IBM DB2 DAS 权限提升漏洞、IBM DB2 XML 功能信息泄露漏洞、IBM DB2 XML 功能拒绝服务漏洞、IBM WebSphere Application Snoop Servlets 信息泄露漏洞、IBM WebSphere Sensor Events 目录遍历漏洞等。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=50350
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=50349
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=50345
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=50339
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=50341
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=50056
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=50346
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=50347

4、Ubuntu 安全漏洞

Ubuntu 是一款基于 Linux 内核的操作系统。本周，该产品被披露存在多个漏洞。攻击者可以利用漏洞通过中间人攻击获取或篡改敏感信息。

CNVD 收录的相关漏洞包括：Ubuntu 'ubuntuone-client'包 SSL 证书验证信息泄露漏洞、Ubuntu 'ubuntu-sso-client'包 SSL 证书验证信息泄露漏洞。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=50300
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=50299

5、Audio Editor Master '.cda 文件处理远程缓冲区溢出漏洞

Audio Editor Master 是一款数字音频编辑器。本周，Audio Editor Master 被披露存在一个综合评级为“高危”的缓冲区溢出漏洞，主要影响 5.4.1.217 版本。攻击者可以利用漏洞构建恶意文件，诱使用户解析，使应用程序崩溃或执行任意代码。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=50295

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-2012-12361	WHMCompleteSolution 存在未明 SQL 注入漏洞	高	用户可参考如下供应商提供的安全公告获得补丁信息: http://go.whmcs.com/26/secpatch
CNVD-2012-12412	SyndeoCMS 'newsletter_email'参数 SQL 注入漏洞	高	暂无
CNVD-2012-12326	Network UPS Tools (NUT) 'addchar()'函数缓冲区溢出漏洞	高	用户可参考如下供应商提供的安全公告获得补丁信息: http://trac.networkupstools.org/projects/nut/browser/trunk/common/parseconf.c?rev=3633
CNVD-2012-12414	Wordpress 插件 Font Uploader 任意文件上传漏洞	高	暂无
CNVD-2012-12341	ZTE Score M 手机硬编码漏洞	高	用户可参考如下供应商提供的安全公告获得补丁信息: http://www.zte.com.cn/cn/
CNVD-2012-12393	Nmedia Users File Uploader 插件任意文件上传漏洞	高	暂无
CNVD-2012-12328	Ruby on Rails SQL 注入漏洞 (CNVD-2012-12328)	高	用户可参考如下供应商提供的安全公告获得补丁信息: http://weblog.rubyonrails.org/2012/5/31/ann-rails-3-2-4-has-been-released/
CNVD-2012-12388	MyBB 'member.php' SQL 注入漏洞	高	暂无
CNVD-2012-12378	Sielco Sistemi Winlog Lite 缓冲区溢出漏洞	高	暂无
CNVD-2012-12349	Mnews 'view.php' SQL 注入漏洞	高	暂无

表 3 部分高危漏洞列表

小结: 本周, ISC BIND 被披露存在拒绝服务零日漏洞, Ubuntu 和 IBM 的多款产品也被披露存在多个漏洞, 这些漏洞对基础电信运营企业、域名解析服务机构以及网站和企业网络构成较大的威胁。此外, Mozilla 产品被披露存在的多个安全漏洞以及 Audio Editor Master 软件存在的零日漏洞, 也需引起政府、企业和个人用户重视, 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、Microsoft 发布升级程序，修补 Windows 安全漏洞

Microsoft Windows 是一款操作系统。本周，Microsoft 发布升级程序，修补了 Windows 存在的漏洞。攻击者可以利用漏洞对代码进行未经授权签名，发起钓鱼，内容伪造，中间人等攻击。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/sites/main/preview/bdgg_preview.htm?tid=17752

本周要闻速递

1. 微软 6 月将发布 7 个补丁修复 28 个安全漏洞

6 月 8 日消息，微软将发布 7 个安全补丁，修复 28 个安全漏洞。这些安全漏洞涉及到 Windows、IE 浏览器、Visual Basic for Applications、Dynamics AX 和 .NET 框架等微软产品。在这 7 个安全补丁中，有 3 个安全补丁是“严重”等级的，涉及到 Windows、IE 浏览器和 .NET 框架。其余 4 个安全补丁是“重要”等级的。利用这些安全漏洞可实施执行代码攻击和提升权限攻击。

参考链接：http://news.ccidnet.com/art/946/20120608/3937019_1.html

2. 黑客利用火狐严重漏洞盗取用户密码

火狐浏览器刚刚发现的一个漏洞可以让黑客很容易就偷走用户在自己网页上留下的信息，例如在 MySpace.com 上留下的用户资料。这个漏洞存在于火狐用户登录管理系统，可以将用户的登录信息发送到攻击者指定的网页。根据这个项目开发时的测试数据库留下的目录，火狐的开发者将这个漏洞定义为危急级别。这个漏洞之所以出现，是因为当用户开始登录时，火狐的登录管理器没有一个足够彻底的检查去决定到底是否要发送这个信息，而且不能确定这个通行证信息是否发送到被要求的服务器。微软的 IE 同样也容易受到这些类型攻击的影响，像火狐一样，它不能确定所提交的用户信息是否发送到了被请求的页面。

参考链接：<http://www.pcpop.com/doc/0/803/803065.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