

信息安全漏洞周报

2012 年 5 月 28 日-2012 年 6 月 3 日

2012 年第 22 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 33 个、中危漏洞 62 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 97 个。本周收录的漏洞中，已有 53 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“Microsoft Wordpad '.doc'文件空指针引用拒绝服务漏洞”、“WHMCS 'boleto_bb.php' SQL 注入漏洞”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 6 家成员单位和多个合作伙伴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，恒安嘉新、启明星辰、天融信、安天实验室等单位报送数量较多。此外，恒安嘉新、上海交通大学以及多位个人漏洞研究者向 CNVD 提交了 18 个原创漏洞。

报送单位或个人	漏洞报送数量	原创漏洞数量
恒安嘉新	51	5
启明星辰	48	0
安天实验室	29	0
天融信	15	0
安氏领信	2	0
东软	1	0
上海交通大学	9	9
个人报送者	4	4
报送总计	159	18

总计	101（去重）	18
----	---------	----

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Drupal、Wordpress、Whmcs、Cisco、Microsoft 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	Drupal	13	13%
2	Wordpress	4	4%
3	Whmcs	3	3%
4	Linux	2	2%
5	Asterisk	2	2%
6	Vmware	1	1%
7	Sony	1	1%
8	Microsoft	1	1%
9	Cisco	1	1%
10	Python	1	1%
11	其它	72	71%

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 101 个漏洞。其中操作系统漏洞 2 个，应用程序漏洞 50 个，WEB 应用漏洞 47 个，网络设备漏洞 2 个。

漏洞影响对象类型	漏洞数量
操作系统漏洞	2
应用程序漏洞	50
WEB 应用漏洞	47
网络设备漏洞	2
数据库漏洞	0
安全产品漏洞	0

表 3 漏洞按影响类型统计表

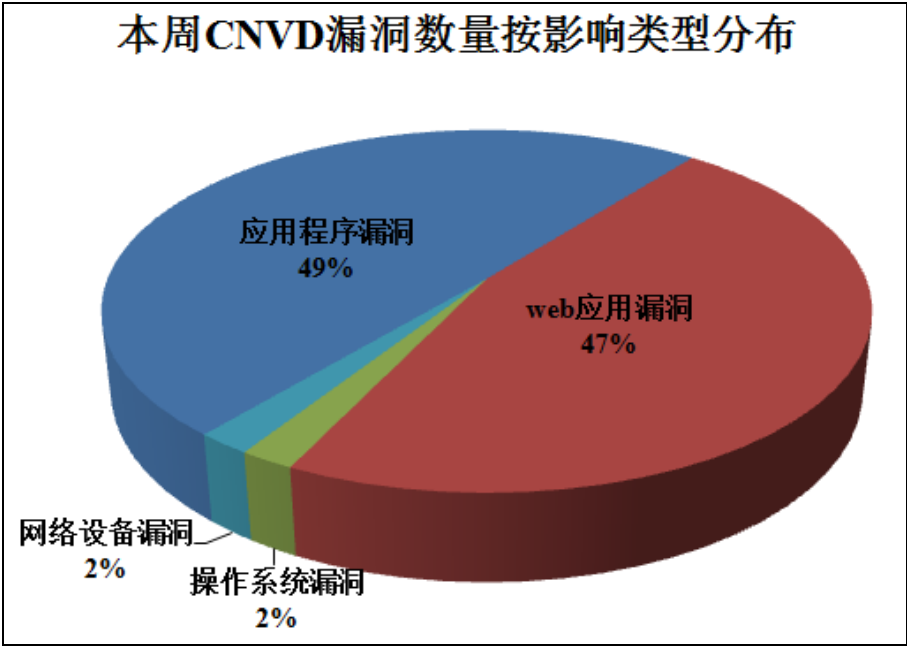


图 1 本周漏洞按影响类型分布

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，“Cisco IOS XR 路由处理器拒绝服务漏洞”和“Logitec 多个 LAN-W300N 产品安全绕过漏洞”。上述漏洞的综合评级均为“高危”。

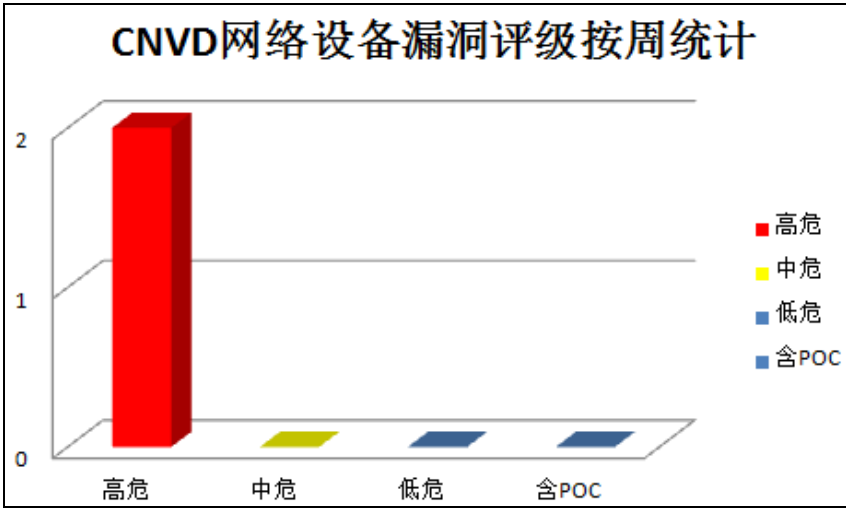


图 2 网络设备漏洞统计

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 Wordpad '.doc'文件空指针引用拒绝服务漏洞

Microsoft Wordpad 是 Windows 操作系统中自带的写字板程序。本周，该程序被披露存在一个拒绝服务漏洞。由于应用程序未能正确处理'.doc'文件，可触发空指针引用，攻击者可以构建恶意文件，诱使用户解析，使应用程序崩溃。

CNVD 对该漏洞的综合评级为“中危”。目前，互联网上已经出现了针对该漏洞的攻击代码，主要影响 Microsoft WordPad 5.1 版本。微软公司尚未发布该漏洞的修补程序。CNVD 提醒广大 Microsoft 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=49977

2、Cisco IOS XR 路由处理器拒绝服务漏洞

Cisco IOS XR 是 Cisco IOS 软件家族的一员。本周，该 Cisco 产品被披露存在一个拒绝服务漏洞，当系统在处理特制报文时可触发此拒绝服务漏洞。此漏洞存在于 Cisco 9000 Series Aggregation Services Routers (ASR) Route Switch Processor (RSP440)和 Cisco Carrier Routing System (CRS) Performance Route Processor (PRP) 上。

CNVD 对该漏洞的综合评级为“高危”。目前，厂商已经发布了该漏洞的修复程序。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/sites/main/preview/ldgg_preview.htm?tid=49758

3、Drupal 模块安全漏洞

Drupal 是使用 PHP 语言编写的开源内容管理框架(CMF)，它由内容管理系统(CMS)和 PHP 开发框架(Framework)共同构成。本周，Drupal 的多个模块被披露存在多个安全漏洞，攻击者可以利用漏洞进行跨站请求伪造、跨站脚本、SQL 注入等攻击，从而绕过安全限制，获得敏感信息或执行任意代码。

CNVD 收录的相关漏洞包括：Drupal BrowserID 模块跨站请求伪造漏洞、Drupal BrowserID 模块安全绕过漏洞、Drupal Amadou 模块跨站脚本漏洞、Drupal Mobile Tools 模块存在多个 HTML 注入漏洞、Drupal Counter 模块 SQL 注入漏洞。其中，“Drupal Counter 模块 SQL 注入漏洞”的综合评级为“高危”，且厂商尚未发布修补程序。其余漏洞均已被修补，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=49836

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=49795

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=49796

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=50016

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=50015

4、VMware vMA 本地权限提升漏洞

VMWare vMA (vSphere Management Assistant) 是一个 VMWare 虚拟机远程命令行终端，用户通过它可以向 ESX 或 ESXi 主机发送命令。本周，该产品被披露存在一个本地权限提升漏洞。由于程序在装载库时存在未明错误，本地攻击者利用漏洞提升权限。

CNVD 对该漏洞的综合评级为“中危”。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=49418

5、WHMCS 产品安全漏洞

WHMCS 是一套专为主机业务及其他在线交易开发的客户管理和财务支持软件。本周，该产品被披露存在多个零日漏洞。攻击者可利用漏洞在受影响的系统中进行 SQL 注入、跨站脚本攻击，获得数据库敏感信息、控制应用系统或执行任意代码。

CNVD 收录的相关漏洞包括：WHMCS 跨站脚本漏洞、WHMCS 存在多个 HTTP 参数漏洞、WHMCS 'boleto_bb.php' SQL 注入漏洞。其中，“WHMCS 'boleto_bb.php' SQL 注入漏洞”的综合评级为“高危”。目前，互联网上已经出现了针对上述漏洞的攻击代码，且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=49538

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=50018

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=50017

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-2012-12321	Segue SQL 注入漏洞	高	暂无
CNVD-2012-12309	Ruby on Rails Active Record SQL 注入漏洞	高	Ruby on Rails 3.2.4, 3.1.5 和 3.0.13 已经修复此漏洞，建议用户下载使用： http://www.rubyonrails.com/
CNVD-2012-12310	Sorensoft Power Media '.asz'文件缓冲区溢出漏洞	高	暂无
CNVD-2012-12281	VAMCart 'tinybrowser.php'任意文件上传漏洞	高	暂无
CNVD-2012-12279	Sony VAIO Wireless Manager ActiveX 控件'WifiMan.dll'缓冲区溢出漏洞	高	Sony 建议用户使用 VAIO 更新，安装此软件的最新版本： http://esupport.sony.com/US/perl/support-info.pl?template_id=1
CNVD-2012-12123	Serendipity 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://blog.s9y.org/archives/241-Seren

			dipity-1.6.2-released.html
CNVD-2012-12112	bsnes '.nes'文件缓冲区溢出漏洞	高	暂无
CNVD-2012-12116	ResEdit PE 文件处理缓冲区溢出漏洞	高	暂无
CNVD-2012-12114	Logitech 多个 LAN-W300N 产品安全绕过漏洞	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.logitech.co.jp/info/2012/0516.html?link_id=out_oshirase_20120516_2_2
CNVD-2012-12113	dotCMS 任意代码执行漏洞	高	dotCMS 2.0.1 和 1.9.5.1 已经修复此漏洞，建议用户下载使用： http://www.dotcms.org/

表 3 部分高危漏洞列表

小结：本周，Microsoft Wordpad 被披露存在拒绝服务零日漏洞，攻击者可以构建恶意文件，诱使用户解析，使应用程序崩溃。目前，互联网已经出现针对该漏洞的攻击代码。Cisco IOS XR 路由处理器也被披露存在拒绝服务漏洞，攻击者可以利用漏洞对相关现网设备发起拒绝服务攻击。另外，VMWare vMA 本地权限提升漏洞，Drupal 多个模块存在的多个安全漏洞，WHMCS 软件零日漏洞也对使用上述产品的企业和个人用户造成较为严重的威胁。

CNVD 提醒使用相关产品的用户注意加强防范。

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、Sony 发布升级程序，修补 VAIO Wireless Manager 安全漏洞

Sony VAIO Wireless Manager 是索尼笔记本上安装的无线管理程序。本周，Sony 发布升级程序，修补了 VAIO Wireless Manager 存在的漏洞。攻击者可以利用漏洞以应用程序上下文执行任意代码。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=17531

本周要闻速递

1. Facebook 悬赏发现其网站漏洞的黑客

据 Facebook 安全响应团队主管赖安·麦克吉汗（Ryan McGeehan）称，Facebook 已经向发现其网站漏洞并帮助修复的黑客们支付了超过 30 万美元的金额。5 月初，麦克吉汗在美国知名问答网站 Quora 上的一篇帖子中透露，Facebook 的漏洞奖金项目自去年 7 月启动以来，已经向 27 个国家的 131 名黑客支付了奖金，还聘请了其中一位作为暑期实习生。该项目通常为每个报告给 Facebook 安全团队的漏洞支付大约 1,000 美元的奖金。

“奖金是对公司责任披露政策（该政策已存在多年）的强调，”麦克吉汗写道，“根据漏洞奖金项目提供的数据，我们已经做了几次全网改进，整体来说这个项目是具有成本效益的，并合理地报答了研究者。通常情况下，我们支付的比最低奖金（500 美元）多很多，并且在很多情况下，对这个为 Facebook 做出贡献并日益全球化的研究者群体增加投入变得越来越有意义。”

参考链接：<http://www.hackbase.com/news/2012-06-04/112964.html>

2. 英国研究员发现波音 787 客机电子系统存漏洞

据英国媒体 5 月 29 日报道，英国剑桥大学研究员谢尔盖·斯科罗博加托夫和库欧·瓦迪斯实验室研究员克里斯·伍兹日前表示，他们发现波音 787 客机以及一些军用设备的电子系统存在严重安全漏洞。29 日，两位研究员向英国媒体展示了他们的一份研究报告的草稿。该报告显示，黑客可以利用上述安全漏洞，很容易控制波音 787 客机上的一块电脑芯片，并进行其他操作。这块芯片是由美国爱特公司制造的，而且两位研究者怀疑，它上面的“后门”正是爱特公司故意预留的。。

参考链接：<http://news.sina.com.cn/o/2012-05-31/032024508494.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