

信息安全漏洞周报

2012 年 5 月 21 日-2012 年 5 月 27 日

2012 年第 21 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 115 个，其中高危漏洞 32 个、中危漏洞 77 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 107 个。本周收录的漏洞中，已有 73 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“FreeNAC SQL 注入漏洞”、“PHP 'com_print_typeinfo()' 远程代码执行漏洞”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 115 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、天融信、恒安嘉新、安天实验室等单位报送数量较多。此外，知道创宇、奇虎 360、网御星云、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。（注：奇虎 360 公司报送了 3 个疑似漏洞，目前确认 1 个）。

报送单位或个人	漏洞报送数量	原创漏洞数量
绿盟科技	43	0
天融信	80	0
启明星辰	78	0
恒安嘉新	24	0
安天实验室	24	0
知道创宇	1	1
东软	4	0
奇虎 360	1	1

网御星云	1	1
上海交通大学	6	6
个人报送者	9	9
报送总计	271	18
总计	115（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 Google、Moodle、WordPress、RT 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	Google	13	11.3%
2	Moodle	13	11.3%
3	WordPress	9	7.8%
4	RT	7	6.1%
5	Microsoft	4	3.5%
6	Symantec	4	3.5%
7	Linux	3	2.6%
8	FreeNAC	3	2.6%
9	Wireshark	3	2.6%
10	Ruubik	3	2.6%
11	其它	53	46.1%

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 115 个漏洞。其中操作系统漏洞 6 个，应用程序漏洞 74 个，WEB 应用漏洞 35 个。

漏洞影响对象类型	漏洞数量
操作系统漏洞	6
应用程序漏洞	74
WEB 应用漏洞	35
网络设备漏洞	0
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

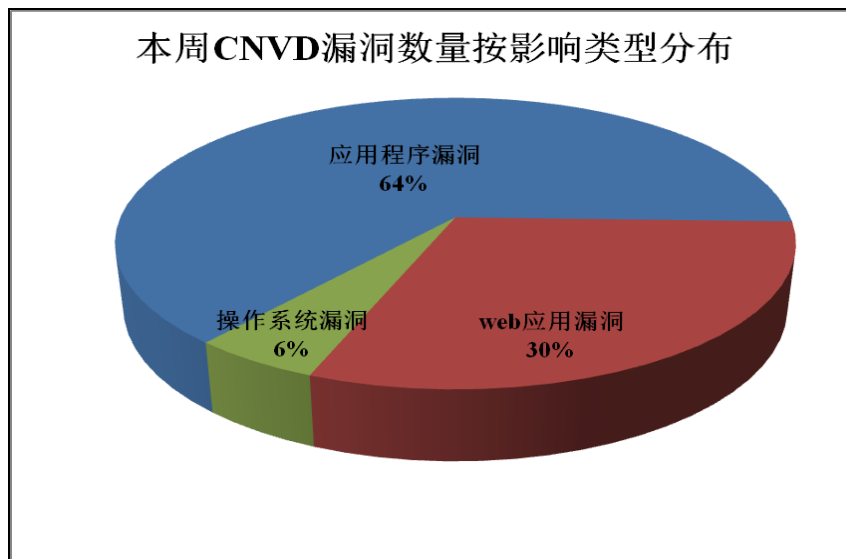


图 1 本周漏洞按影响类型分布

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、Google Chrome 安全漏洞

Google Chrome 是一款开源的 WEB 浏览器。本周，Google Chrome 被披露存在多个安全漏洞，攻击者可以利用漏洞，发起拒绝服务攻击或执行任意代码。CNVD 收录的相关漏洞包括：Google Chrome v8 垃圾收集拒绝服务漏洞、Google Chrome first-letter 处理内存错误引用漏洞、Google Chrome websocket 处理内存破坏漏洞、Google Chrome PDF 处理越界写漏洞、Google Chrome PDF 色彩空间处理漏洞、Google Chrome PDF 函数缓冲区溢出漏洞、Google Chrome 插件 Javascript 绑定漏洞、Google Chrome V8 类型破坏漏洞等。上述漏洞的综合评级均为“高危”。目前，厂商已经发布这些漏洞的修补程序。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/sites/main/preview/ldgg_preview.htm?tid=49275
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=49278
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=49279
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=49287
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=49290
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=49291
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=49281
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=49292

2、Moodle 安全漏洞

Moodle 是一款开源的网络教学应用程序。本周，Moodle 被披露存在多个安全漏洞，攻击者可以利用漏洞窃取敏感信息或控制应用系统。CNVD 收录的相关漏洞包括：

Moodle SQL 注入漏洞、Moodle 跨站脚本漏洞（CNVD-2012-11993）、Moodle 安全绕过漏洞（CNVD-2012-11994）、Moodle 隐藏信息泄露漏洞、Moodle 测验权限检查漏洞、Moodle 题库访问漏洞、Moodle 用户权限修改漏洞、Moodle 数据库活动模块写访问漏洞等。其中，“Moodle SQL 注入漏洞”的综合评级为“高危”。目前，厂商已经发布了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/sites/main/preview/ldgg_preview.htm?tid=49135
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=49115
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=49116
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=49117
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=49123
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=49124
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=49129
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=49134

3、Request Tracker 安全漏洞

Request Tracker（RT）是一款企业级的问题跟踪系统。本周，该产品被披露存在多个安全漏洞，攻击者可以利用漏洞构建恶意链接，执行任意代码或控制应用系统。CNVD 收录的相关漏洞包括：RT 信息泄露漏洞、RT SQL 注入漏洞、RT ticket 信息泄露漏洞、RT 跨站脚本漏洞、RT 权限提升漏洞、RT 任意代码执行漏洞、RT 跨站请求伪造漏洞。其中，“RT SQL 注入漏洞”的综合评级为“高危”。目前，厂商已经发布这些漏洞的修补程序。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/sites/main/preview/ldgg_preview.htm?tid=49217
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=49218
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=49220
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=49227
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=49222
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=49225
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=49224

4、IBM 产品安全漏洞

IBM Lotus Quickr 是一款 IBM 开发的协同文档工具；IBM Rational Change 是一款基于 Web 的整合式变更控制和管理解决方案。本周，上述产品被披露存在多个安全漏洞，攻击者可以利用漏洞获取敏感信息，执行任意代码。CNVD 收录的相关漏洞包括：IBM Lotus Quickr 'qp2.cab' ActiveX 控件栈缓冲区溢出漏洞、IBM Rational Change 跨站脚本漏洞。其中，“IBM Lotus Quickr 'qp2.cab' ActiveX 控件栈缓冲区溢出漏洞”的综合评级为“高危”。目前，厂商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/sites/main/preview/ldgg_preview.htm?tid=49099

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=49282

5、FreeNAS SQL 注入漏洞

FreeNAS 是一套免费的 NAS 服务软件。本周，FreeNAS 被披露存在一个综合评级为“高危”的 SQL 注入漏洞，主要影响 3.02 版本。攻击者可利用此漏洞在受影响的系统中发起注入攻击，获得后台数据库信息或执行任意代码。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=49198

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-2012-12098	Jaow CMS SQL 注入漏洞	高	供应商发布了安全公告及相关补丁信息，修复了此漏洞，建议用户下载使用。避免攻击者可以利用漏洞进行 SQL 注入攻击，可获得数据库敏感信息或控制应用系统： http://www.jaow.net/Article-97
CNVD-2012-12095	EMC AutoStart 存在多个缓冲区溢出漏洞	高	供应商发布了安全公告及相关补丁信息，修复了此漏洞，建议用户下载使用。避免成功利用漏洞可使应用程序崩溃或以应用程序上下文执行任意代码： http://www.emc.com/products/detail/software/autostart.htm
CNVD-2012-12057	BlackArmor 网络管理员密码重置安全绕过漏洞	高	暂无
CNVD-2012-12059	appRain CMF 'uploadify.php'远程任意文件上传漏洞	高	暂无
CNVD-2012-12100	Measuresoft ScadaPro DLL 装载任意代码执行漏洞	高	供应商发布了安全公告及相关补丁信息，修复了此漏洞，建议用户下载使用。避免导致以应用程序上下文执行任意代码： http://www.measuresoft.net/download/versions.aspx?v=CB
CNVD-2012-12066	SuperNews SQL 注入漏洞	高	暂无

CNVD-2012-12025	HAProxy Trash 缓冲区溢出漏洞	高	供应商发布了安全公告及相关补丁信息，修复了此漏洞，建议用户下载使用。避免需要 global.tune.bufsize 配置选项设置的值大于默认值，并且配置了 header 重写(通过 reqrep 或 rsprep 配置指令): http://haproxy.1wt.eu/
CNVD-2012-12055	Adiscon LogAnalyzer SQL 注入漏洞	高	供应商发布了安全公告及相关补丁信息，修复了此漏洞，建议用户下载使用。避免攻击者可以利用漏洞获得数据库敏感信息或控制应用程序： http://loganalyzer.adiscon.com
CNVD-2012-12000	activeCollab 聊天模块任意 PHP 代码执行漏洞	高	供应商发布了安全公告及相关补丁信息，修复了此漏洞，建议用户下载使用。避免远程攻击者可以利用漏洞以应用程序上下文执行任意 PHP 代码： http://www.uswebstyle.com/activecollab.html
CNVD-2012-12066	SuperNews SQL 注入漏洞	高	暂无

表 3 部分高危漏洞列表

小结：本周，Google Chrome 浏览器被披露存在漏洞，攻击者可以利用漏洞构建恶意文件，导致应用程序崩溃或执行任意代码。Moodle 和 Request Tracker 系统以及 IBM 的两款产品也分别被披露存在多个漏洞，攻击者可以利用漏洞窃取敏感信息、执行任意代码或控制应用系统。此外，FreeNAS 网络存储服务软件被披露存在零日漏洞。上述产品由于采用的企业和个人用户较多，需引起重视，加强防范。

请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、Linux 发布升级程序，修补 Kernel 安全漏洞

Linux 是一款开源的操作系统。本周，Linux 发布升级程序，修补了 Kernel 存在的多个漏洞。远程或本地的攻击者可以利用漏洞发起拒绝服务攻击或执行任意代码。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=17296
http://www.cnvd.org.cn/sites/main/preview/bdgg_preview.htm?tid=17176
http://www.cnvd.org.cn/sites/main/preview/bdgg_preview.htm?tid=17178



本周要闻速递

1. 微软修补 Duqu 木马幽灵漏洞

近日，微软发布了一个综合的更新文件来修补与 Duqu 恶意软件有关的字体解析代码漏洞，解决了在 Office 产品、Windows 系统和 .NET 框架中的一些严重缺陷。微软发布了 7 个安全公告、其中 3 个评级为“严重”，共修补产品线的 23 个漏洞。自从去年 11 月以来这是微软第 2 次更新受 Duqu 木马影响的软件。

参考链接：<http://security.ctocio.com.cn/44/12343544.shtml>

2. OpenOffice 漏洞已修复

根据国外媒体报道，最新版本的开源办公套件 Apache OpenOffice 3.4.0，目前已经解决了此前发现的安全漏洞，并且对漏洞进行了详细说明。之前发布的 Apache OpenOffice 3.4.0，包括针对 3 个安全漏洞的更新包，这些更新包都被列为“important”级别。这三个漏洞涉及处理内置图片时产生的整数溢出错误、导入 WordPerfect 文件产生的内存重写 bug 等。这两项漏洞都可被用来注入恶意代码，为黑客假扮身份打开 booby-trapped 文件提供条件。另外一个漏洞主要是在处理复杂的 PPT 文件的时候，产生严重的程序崩溃 bug。目前，OpenOffice.org 3.3 和 OpenOffice.org 3.4 beta 版本都受这些漏洞影响，而最新版本 Apache OpenOffice 3.4.0 已经彻底解决这类问题，它也是基于全新管理平台下首次被发布的办公软件。

参考链接：<http://article.pchome.net/content-1505641.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

邮箱：vreport@cert.org.cn

电话：010-82990999