

信息安全漏洞周报

2012 年 6 月 18 日-2012 年 6 月 24 日

2012 年第 25 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 102 个，其中高危漏洞 41 个、中危漏洞 54 个、低危漏洞 7 个。上述漏洞中，可利用来实施远程攻击的漏洞有 89 个。本周收录的漏洞中，已有 57 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“Sysax Multi Server 'scriptpathbrowse2.htm'缓冲区溢出漏洞”、“Wordpress 插件 Newsletter 目录遍历漏洞”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 102 个漏洞。各单位报送情况如表 1 所示。其中，启明星辰、天融信、恒安嘉新、绿盟科技、安天实验室等单位报送数量较多。此外，知道创宇、广西网信、上海交通大学以及 6 位个人漏洞研究者向 CNVD 提交了 31 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	52	0
天融信	34	0
恒安嘉新	32	0
绿盟科技	27	0
安天实验室	22	0
安氏领信	5	0
东软	3	0
知道创宇	1	1

个人报送者	8	8
上海交通大学	19	19
广西网信	3	3
报送总计	206	31
总计	102（去重）	31

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、IBM、Joomla!、Linux 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	11	11%
2	IBM	9	9%
3	Joomla!	7	7%
4	Linux	6	6%
5	Siemens	5	5%
6	e107	5	5%
7	XnView	3	3%
8	USWebStyle	3	3%
9	Oracle	3	3%
10	Cisco	3	3%
11	其它	47	45%

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 102 个漏洞。其中操作系统漏洞 7 个，应用程序漏洞 48 个，WEB 应用漏洞 42 个，数据库漏洞 1 个，安全产品漏洞 4 个。

漏洞影响对象类型	漏洞数量
操作系统漏洞	7
应用程序漏洞	48
WEB 应用漏洞	42
网络设备漏洞	0
数据库漏洞	1
安全产品漏洞	4

表 3 漏洞按影响类型统计表

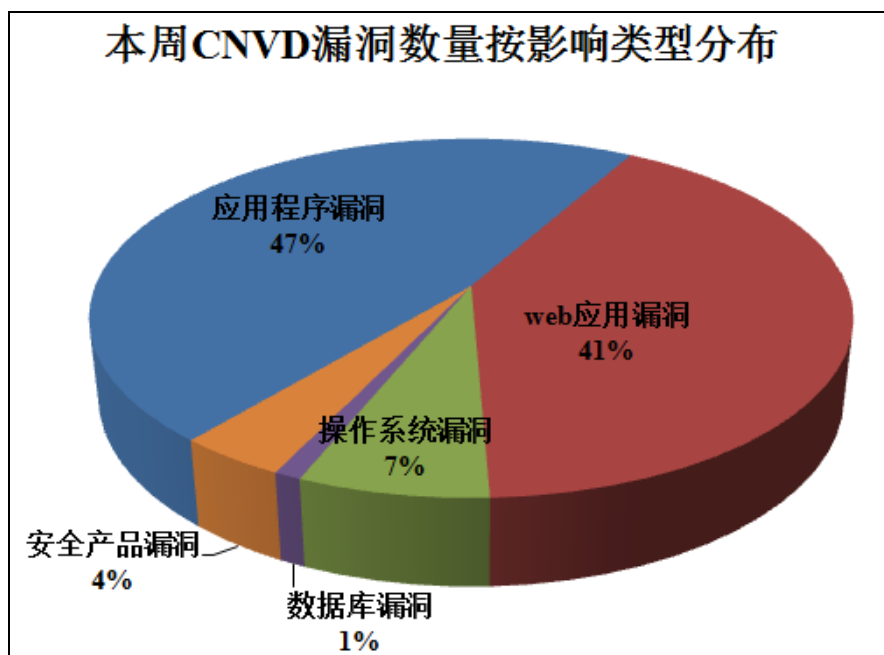


图 1 本周漏洞按影响类型分布

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、VMWare 产品漏洞

VMWare 是一款虚拟机软件。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在主机上执行任意代码或使虚拟机崩溃。

CNVD 收录的相关漏洞包括：VMware Workstation、Player、Fusion、ESXi、ESX Checkpoint 文件解析漏洞（CNVD-2012-12559）、VMware Workstation、Player、Fusion、ESXi、ESX Checkpoint 文件解析漏洞（CNVD-2012-12560）。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=50775

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=50755

2、Linux Kernel 安全漏洞

Linux Kernel 是 Linux 操作系统的内核。本周，该产品被披露存在多个安全漏洞，攻击者可利用此漏洞触发内核崩溃，造成拒绝服务攻击或提升权限。

CNVD 收录的相关漏洞包括：Linux Kernel Reliable Datagram Sockets (RDS) 本地拒绝服务漏洞（CNVD-2012-12573）、Linux Kernel KVM 'kvm_set_irq()'函数本地缓冲区溢出漏洞、Linux Kernel DRM 子系统整数溢出漏洞（CNVD-2012-12571）、Linux Kernel DRM 子系统整数溢出漏洞、Linux Kernel 未过滤 netdev rio_ioctl 访问漏洞、Linux Kernel EXT4 'ext4_fill_flex_info()'本地拒绝服务漏洞。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=50807
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=50806
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=50805
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=50804
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=50803
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=50677

3、Oracle 产品安全漏洞

Sun Java Runtime Environment 主要为 JAVA 应用程序提供可靠的运行环境。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获得敏感信息，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：Oracle Java Runtime Environment 组件拒绝服务漏洞、Oracle Java Runtime Environment 组件信息泄露漏洞、Oracle JavaFX 2D 远程代码执行漏洞。其中，“Oracle JavaFX 2D 远程代码执行漏洞”的综合评级为“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=50721
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=50722
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=50720

4、Cisco 产品安全漏洞

Cisco Adaptive Security Appliance 是一款自适应安全设备，用于提供安全和 VPN 服务；Cisco AnyConnect Secure Mobility 是一款安全的企业移动解决方案。本周，上述产品被披露存在多个漏洞。远程攻击者可以利用漏洞绕过管理员的访问限制，读取或修改配置设置。

CNVD 收录的相关漏洞包括：Cisco ASA 5500/Cisco Catalyst 6500 系列拒绝服务漏洞、Cisco AnyConnect Secure Mobility Client/Cisco Secure Desktop HostScan 软件降级漏洞、Cisco AnyConnect Secure Mobility Client 软件降级漏洞。其中，“Cisco ASA 5500/Cisco Catalyst 6500 系列拒绝服务漏洞”的综合评级为“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=50878
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=50877
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=50876

5、Sysax Multi Server 'scriptpathbrowse2.htm'缓冲区溢出漏洞

Sysax Multi Server 是一款 windows 平台下的 SSH2 和 FTP 服务器软件。本周，Sysax Multi Server 被披露存在一个综合评级为“高危”的缓冲区溢出漏洞。攻击者可以利用

漏洞执行任意代码。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=50887

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-2012-12586	WordPress 插件 Zingiri Web Shop 任意文件上传漏洞	高	暂无
CNVD-2012-12567	Rack::Cache rubygem 信息泄露漏洞	高	用户可参考如下供应商提供的安全公告获得补丁信息： https://github.com/rtomayko/rack-cache/commit/2e3a64d07daac4c757cc57620f2288e865a09b90
CNVD-2012-12581	Joomla! Dione FileUploader 模块任意文件上传漏洞	高	暂无
CNVD-2012-12575	WordPress 插件 Automatic 'q' SQL 注入漏洞	高	供应商已发布补丁修复了此漏洞： http://codecanyon.net/item/wordpress-automatic-plugin/1904470
CNVD-2012-12579	WordPress 插件 Lim4wp 任意文件上传漏洞	高	暂无
CNVD-2012-12566	Innominate Security Technologies mGuard 不充分熵漏洞	高	Innominate mGuard 7.5.0 已经修复此漏洞，建议用户下载使用： http://www.innominate.com/data/downloads/software/innominate_security_advisory_20120614_001.pdf
CNVD-2012-12562	ESRI ArcMap 'mxd'文件任意代码执行漏洞	高	暂无
CNVD-2012-12550	XnView ECW 图像处理漏洞	高	供应商已发布补丁修复了此漏洞： http://www.xnview.com
CNVD-2012-12583	Simple Document Management System 存在多个 SQL 注入漏洞	高	暂无
CNVD-2012-12551	XnView RAS 图像处理漏洞	高	供应商已发布补丁修复了此漏洞： http://www.xnview.com

表 3 部分高危漏洞列表

小结：本周，VMWare 产品被披露存在多个漏洞，攻击者利用漏洞可在主机上执行任意代码或使虚拟机崩溃。Linux Kernel 和 Sun Java Runtime Environment 存在的漏洞可被利用发起拒绝服务攻击或执行任意代码。利用 Cisco 产品的漏洞，可绕过管理员的访问限制，读取或修改配置设置。此外，Sysax Multi Server 服务器被披露存在零日漏洞，也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、Siemens 发布升级程序，修补 WinCC flexible 安全漏洞

WinCC flexible 是用在一些机器或流程应用中的人机接口。本周，Siemens 发布升级程序，修补了 WinCC flexible 存在的漏洞。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/sites/main/preview/bdgg_preview.htm?tid=18131
http://www.cnvd.org.cn/sites/main/preview/bdgg_preview.htm?tid=18132
http://www.cnvd.org.cn/sites/main/preview/bdgg_preview.htm?tid=18133
http://www.cnvd.org.cn/sites/main/preview/bdgg_preview.htm?tid=18134
http://www.cnvd.org.cn/sites/main/preview/bdgg_preview.htm?tid=18135

本周要闻速递

1. Windows 出现高危“暴雷”漏洞

上周，微软发布紧急安全公告称，Windows 基础组件出现高危漏洞，影响全版本 IE 浏览器和多版本 Office，几乎全体 Windows 用户均受该漏洞威胁。日前，微软已经发布了相关补丁对该漏洞进行修复。据悉，“暴雷”是基于 Windows XML 基础组件的远程攻击漏洞。利用该漏洞，黑客可以通过恶意网页、文档等形式将任意木马植入用户电脑，窃取重要资料和账号信息。在推出“暴雷”漏洞临时解决方案的同时，微软还发布 7 款正式补丁，用于修复 Windows 系统及软件漏洞。

参考链接：<http://news.sohu.com/20120620/n346116932.shtml>

2. PayPal 宣布将向报告安全漏洞者支付奖金

北京时间 6 月 24 日消息，据国外媒体报道，“有奖捉虫”在美国互联网行业日益普遍，日前，网络支付服务商 PayPal 宣布，将向通过正常渠道报告网站安全漏洞的研究人员支付报酬。据称，有资格获得奖金的安全漏洞类型包括交叉脚本攻击、交叉网站需求伪造、SQL 语句（用于查询后台数据库）注入造假、身份认证绕过等。每一个安全漏洞的奖金数额，将由 PayPal 工作人员具体分析确定。此前，谷歌、Mozilla、Facebook

等公司相继推出了有奖捉虫计划，奖励那些安全研究人员。安全行业人士 Marius Gabriel Avram 评论说，有奖捉虫计划，可以帮助 PayPal 减少网站软件 BUG 数量，但是还不会做到马上消失。这位专家表示，单是在过去两个星期里，他就发现了 PayPal 桌面网站和移动版网站中 10 多个安全漏洞，许多漏洞属于高度危险级别。

参考链接：<http://it.sohu.com/20120624/n346355799.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