

信息安全漏洞周报

2012 年 7 月 9 日-2012 年 7 月 15 日

2012 年第 28 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 105 个，其中高危漏洞 35 个、中危漏洞 64 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 100 个。本周收录的漏洞中，已有 59 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“WordPress Contus Vblog 插件'save.php'任意文件上传漏洞、“Poison Ivy 服务器缓冲区溢出漏洞”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 6 家成员单位和多个合作伙伴报送了本周收录的全部 105 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、绿盟科技、天融信、安天实验室等单位报送数量较多。此外，来自天融信公司、奇虎 360 公司、上海交通大学的漏洞研究者向 CNVD 提交了 4 个原创漏洞或漏洞事件。

报送单位或个人	漏洞报送数量	原创漏洞数量
恒安嘉新	66	0
启明星辰	47	0
绿盟科技	51	0
安天实验室	40	0
天融信	24	1
安氏领信	8	0
上海交通大学	2	2
奇虎 360	1	1
报送总计	240	4

录入总计	105（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、Microsoft、Drupal、Google、Apache 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	20	19%
2	Microsoft	15	10%
3	Drupal	8	7%
4	Google	3	3%
5	Apache	3	3%
6	HP	2	2%
7	Linux	2	2%
8	Check Point	2	2%
9	Joomla!	1	1%
10	IBM	1	1%
11	其它	48	50%

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 105 个漏洞。其中操作系统漏洞 7 个，应用程序漏洞 39 个，WEB 应用漏洞 59 个。本周未收录网络设备、数据库、安全产品等类型的漏洞。

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	39
WEB 应用漏洞	59
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

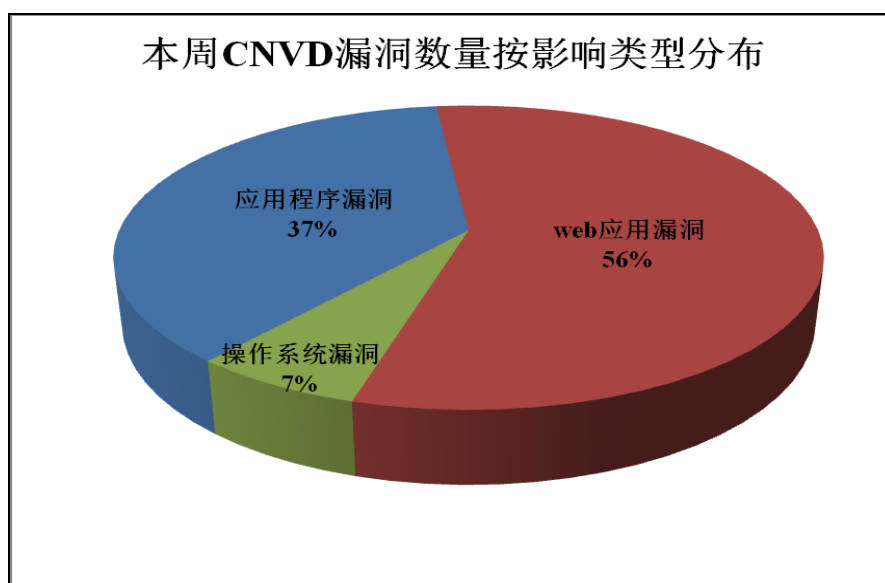


图 1 本周漏洞按影响类型分布

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、Microsoft 产品安全漏洞

7 月 11 日，微软发布了 2012 年 7 月份的月度例行安全公告，共含 9 项更新，修复了涉及 Microsoft Windows、Internet Explorer、Office、开发工具软件和服务器软件等多个产品存在的 16 个安全漏洞。其中，MS12-043、MS12-044 与 MS12-045 项公告的综合评级为最高的“严重”级别，另外 6 项公告则是“重要”级别。利用上述漏洞，攻击者可以远程执行代码，窃取敏感信息或提升特权。

其中，标号为“MS12-043”的安全公告中提及 1 个 IE 浏览器相关的 0day 漏洞。该漏洞由奇虎 360 公司发现并提交 CNVD，CNVD 工作委员会对漏洞情况进行了验证并协调微软公司进行处置。

CNVD 收录的相关漏洞包括：Microsoft Windows 本地特权提升漏洞（CNVD-2012-12956）、Microsoft Windows 文件/目录名处理任意命令注入漏洞、Microsoft SharePoint 跨站脚本漏洞、Microsoft SharePoint HTML 注入漏洞、Microsoft Windows 本地特权提升漏洞（CNVD-2012-12958）、Microsoft Data Access Components 缓冲区溢出漏洞、Microsoft Visual Basic for Applications DLL 装载任意代码执行漏洞、Microsoft Visual Basic for Applications DLL 装载任意代码执行漏洞等。目前，厂商已经发布上述漏洞的修补程序。CNVD 提醒广大 Microsoft 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=51576
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=51581

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=51582

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=51579

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=51578

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=51574

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=51573

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=51568

2、Apache 产品安全漏洞

Hadoop 是 Apache 提供的开放源码并行运算编程工具和分散式数据库系统；Apache HTTP Server 是 Apache 提供的 WEB 应用服务软件；Sling 是基于 Java 内容库（如 Apache Jackrabbit）存储和管理内容的 Web 应用框架。本周，上述产品被披露存在多个安全漏洞，攻击者可利用漏洞对只读权限的数据获得完全的写访问权限或如果可以判断 ID，恶意客户端可以读取该 ID 的任意数据块，发起拒绝服务攻击，消耗大量内存和存储资源。

CNVD 收录的相关漏洞包括：Apache Hadoop 信息泄露漏洞（CNVD-2012-12935）、Apache HTTP Server 'ap_pregsub()'函数本地拒绝服务漏洞、Apache Sling 拒绝服务漏洞（CNVD-2012-12895）。其中，“Apache Hadoop 信息泄露漏洞（CNVD-2012-12935）”的综合评级为“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=51555

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=51501

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=51395

3、WordPress 插件安全漏洞

WordPress 是一款使用 PHP 语言开发的内容管理系统。本周，WordPress 的多款插件被披露存在多个安全漏洞，攻击者可利用通过注入任意 SQL 代码操纵 SQL 查询，上传恶意 PHP 脚本来执行任意 PHP 代码。

CNVD 收录的相关漏洞包括：WordPress 插件 Sendit Newsletter 'id' SQL 注入漏洞、WordPress 插件 Flip Book 任意文件上传漏洞、WordPress 插件 Leaflet Maps Marker SQL 注入漏洞、WordPress Front-end Editor 插件'upload.php'任意文件上传漏洞、WordPress Contus Vblog 插件'save.php'任意文件上传漏洞、WordPress 插件 MoodThingy Mood Rating Widget SQL 注入漏洞等。上述漏洞的综合评级均为“高危”。目前，厂商已经修复了“WordPress 插件 Leaflet Maps Marker SQL 注入漏洞”。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=51564

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=51520

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=51519

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=51497

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=51496

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=51498

4、Linux Kernel 安全漏洞

Linux Kernel 是 Linux 操作系统的内核。本周，Linux Kernel 被披露存在多个漏洞。攻击者利用漏洞可发起拒绝服务攻击，导致系统崩溃。

CNVD 收录的相关漏洞包括：Linux Kernel 密钥管理拒绝服务漏洞、Linux Kernel IPv6 'nf_ct_frag6_reasm()'远程拒绝服务漏洞。其中，“Linux Kernel IPv6 'nf_ct_frag6_reasm()'远程拒绝服务漏洞”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=51571

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=51570

5、Poison Ivy 服务器缓冲区溢出漏洞

Poison Ivy 是一款远端控制工具。本周，Poison Ivy 被披露存在一个栈缓冲区溢出漏洞。远程攻击者可以利用漏洞以应用程序上下文执行任意代码。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=51435

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-2012-12945	Synel SY-780/A 拒绝服务漏洞 (CNVD-2012-12945)	高	暂无
CNVD-2012-12932	VLC Media Player OGG Demuxer 缓冲区溢出漏洞	高	VLC Media Player 2.0.2 版本已修复此漏洞，建议用户下载使用： http://www.videolan.org/vlc/
CNVD-2012-12931	Drupal IMCE Mkdir 'imce'任意文件上传漏洞	高	暂无
CNVD-2012-12897	Pidgin 'mxit_show_message()'栈缓冲区溢出漏洞	高	Pidgin 2.10.5 已经修复此漏洞，建议用户下载使用： http://www.pidgin.im/news/security/index.php?id=64
CNVD-2012-12930	MGB SQL 注入漏洞	高	暂无

CNVD-2012-12911	Forum Oxalis 'id'参数 SQL 注入漏洞	高	暂无
CNVD-2012-12934	Joomla! 'com_szallasok'组件'id'参数 SQL 注入漏洞	高	暂无
CNVD-2012-12995	plow '.plowrc' 文件缓冲区溢出漏洞	高	暂无
CNVD-2012-12999	BookNux SQL 注入漏洞	高	暂无
CNVD-2012-12973	phpLinks 'PID'参数 SQL 注入漏洞	高	暂无

表 3 部分高危漏洞列表

小结：7 月 11 日，微软发布了 2012 年 7 月份的月度例行安全公告，共含 9 项更新，修复了涉及 Microsoft Windows、Internet Explorer、Office、开发工具软件和服务器软件等多个产品存在的 16 个安全漏洞。攻击者利用漏洞可以远程执行代码，窃取敏感信息或提升特权。建议网站管理员和桌面终端用户注意加强防范。

本周，Linux Kernel 和 Apache 的多款产品被披露存在多个漏洞，攻击者利用漏洞发起拒绝服务攻击。多款 WordPress 插件也被披露存在漏洞，攻击者可进行 SQL 注入攻击，上传恶意 PHP 脚本取得服务器管理权限。此外，Poison Ivy 控制工具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、IBM 发布升级程序，修补 WebSphere Portal 安全漏洞

IBM WebSphere Portal 主要用于提供一个组合应用程序或业务 mashup 框架，并提供一种工具来构建基于 SOA 的解决方案。本周，IBM 发布升级程序，修补了 WebSphere Portal 存在的漏洞，允许攻击者通过目录遍历攻击读取任意文件内容。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=18702

注：以上验证信息(方法)可能带有攻击性，仅供安全研究之用。请广大用户加强对漏洞的防范工作，尽快下载相关补丁。

本周要闻速递

1. 甲骨文将发布 88 个安全补丁修复漏洞

7 月 14 日消息，据国外媒体报道，甲骨文计划发布 88 个安全补丁，修复其产品中的广泛的安全漏洞。有 4 个补丁是为甲骨文数据库发布的，其中有 3 个数据库安全漏洞能够被黑客在网络上利用，不需要登录证书。甲骨文还计划为其 Fusion 中间件系列产品发布 22 个补丁，其中有 8 个安全漏洞能够被远程利用，不需要用户名或口令。甲骨文使用 CVSS（通用安全漏洞评分系统）排列其补丁的严重性。其中一个用于 Fusion 中间件产品 JRockit 的补丁的 CVSS 评分是 10.0 分，是严重等级的最高分。另外 25 个补丁修复甲骨文 Sun 系列产品中的安全漏洞，其中包括 GlassFish 应用服务器和 Solaris OS 操作系统。这次发布的补丁还有 6 个用于修复 MySQL 数据库的安全漏洞。这些安全漏洞都不能在没有安全证书的情况下被远程利用。其它补丁修复甲骨文 Hyperion、企业管理器网格控制（Enterprise Manager Grid Control）、电子商务套装软件、Siebel CRM、仁科和甲骨文工业应用（Oracle Industry Applications）等产品中的安全漏洞。

参考链接：http://news.ccidnet.com/art/946/20120714/4052951_1.html

2. 新浪微博出现账号漏洞

7 月 12 日消息，新浪微博昨晚起发生账号错乱，用户反映别人正在使用自己的账号发微博，同时也有用户反映自己登陆微博之后竟然是别人的账号。昨晚，雷锋网官方微博出现恶意刷屏现象，疑似不良人士利用 BUG 所为。其后，多名网友反映遇到类似问题，别人可以使用自己的微博账号发微博，而自己竟然登陆了别人的微博，出现了较大面积账号错乱问题。

参考链接：http://tech.ifeng.com/internet/detail_2012_07/12/15975140_0.shtml

3. Struts2 漏洞拉响网站安全红色警报

中新网 7 月 13 日电，广泛应用在国内大型网站系统的 Struts2 框架正在遭到黑客猛烈攻击。利用 Struts2 “命令执行漏洞”，黑客可轻易获得网站服务器 ROOT 权限、执行任意命令，从而窃取重要数据或篡改网页，目前国内至少有 3500 家网站存在该高危漏洞。据乌云漏洞平台显示，运营商及金融等领域大批网站，甚至包括政府网站均受 Struts2 漏洞影响。据悉，Struts2 “命令执行漏洞”早在 2010 年已经曝光，但当时没有公开的漏洞利用工具，因此并未造成过多危害。直到近期，针对该漏洞新的攻击代码在网上公开，漏洞利用工具也随之涌现，使黑客攻击完全没有门槛，80%以上应用 Struts2 框架的网站因此面临严重风险。之前 Struts2 官方补丁屏蔽了黑客通过\u0023 (16 进制的#) 攻击的方式，但黑客仍可以利用\u002f (8 进制的#) 实施突破。

参考链接：<http://news.sohu.com/20120713/n348116208.shtml>

4. 雅虎 45 万用户密码遭泄露

北京时间 7 月 13 日消息，雅虎证实，大约有 45 万的用户名和密码以及雅虎和其他公司的文件被偷走。一群被称为 D33D 公司的黑客，公布了大约有 453492 个雅虎的用户名和密码。除此之外，他们还公布了包括 Gmail、AOL、Hotmail、Comcast、MSN、SBC Global、Verizon、BellSouth 和 Live.com 用户和密码。黑客是利用软件漏洞，然后

使用 SQL 注入的方法盗取了密码。为了避免进一步伤害，其他的二级域名和易受攻击的参数尚未发布。目前还不清楚雅虎是否已经修复了漏洞，黑客可能仍然在系统内，因此雅虎用户在其他网站有使用相同账户和密码的话，应该更改其他相同的密码。

参考链接：<http://news.sxpmg.com/ynxx/szcb/201207/95167.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