

信息安全漏洞周报

2012 年 7 月 23 日-2012 年 7 月 29 日

2012 年第 30 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**高**。

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 195 个，其中高危漏洞 98 个、中危漏洞 82 个、低危漏洞 15 个。上述漏洞中，可利用来实施远程攻击的漏洞有 184 个。本周收录的漏洞中，已有 175 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“PHP 'openssl_verify()'缓冲区溢出漏洞”、“httpdx 通配符拒绝服务漏洞”、“PHPCMS v9 文件包含漏洞”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 1 个合作伙伴报送了本周收录的全部 195 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、安天实验室等单位报送数量较多。此外，恒安嘉新、凌迅网络、上海交通大学以及个人报送者向 CNVD 提交了 7 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	131	0
绿盟科技	120	0
安天实验室	101	0
恒安嘉新	5	1
天融信	25	0
安氏领信	14	0
东软	4	0
凌迅网络	2	2

个人报送者	1	1
上海交通大学	3	3
报送总计	406	7
录入总计	195（去重）	7

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Apple、Oracle、Symantec、ISC 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	Apple	76	39%
2	Oracle	53	27%
3	Symantec	6	3%
4	ISC	5	2%
5	Wordpress	5	2%
6	Caucho Technology	5	2%
7	PHP	3	1%
8	IBM	2	1%
9	JBoss	1	1%
10	Cisco	1	1%
11	其它	38	21%

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 195 个漏洞。其中操作系统漏洞 12 个，应用程序漏洞 157 个，WEB 应用漏洞 12 个，数据库漏洞 7 个，网络设备漏洞 7 个。

漏洞影响对象类型	漏洞数量
操作系统漏洞	12
应用程序漏洞	157
WEB 应用漏洞	12
网络设备漏洞	7
数据库漏洞	7
安全产品漏洞	0

表 3 漏洞按影响类型统计表

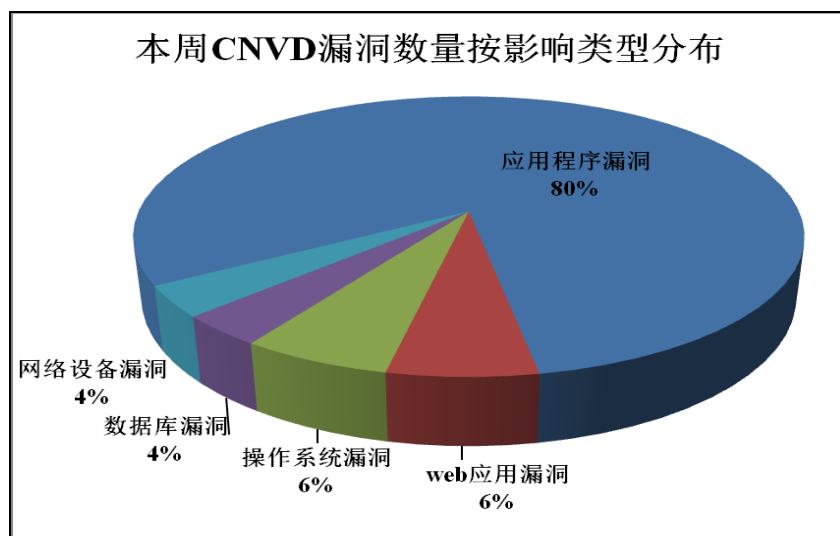


图1 本周漏洞按影响类型分布

本周涉及电信行业漏洞信息

本周，CNVD 收录了 7 个网络设备漏洞。其中，“Symantec Web Gateway shell 命令执行漏洞、Symantec Web Gateway 代码注入漏洞、Symantec Web Gateway 本地文件操作验证绕过漏洞、Symantec Web Gateway SQL 注入漏洞、Symantec Web Gateway SQL 盲注漏洞、Symantec Web Gateway 密码更改安全绕过漏洞”的综合评级均为“高危”，“Cisco Linksys WMB54G 远程命令注入漏洞”的综合评级均为“中危”。

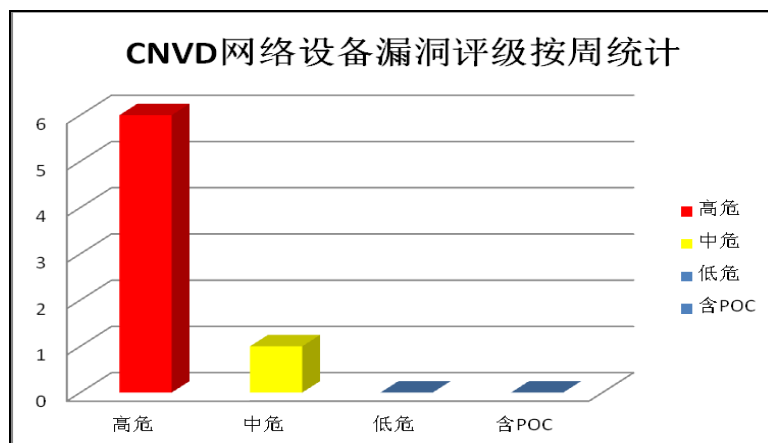


图2 网络设备漏洞统计

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、Apple Safari 安全漏洞

Apple Safari 是一款 WEB 浏览器。本周，该产品被披露存在多个安全漏洞，攻击

者利用漏洞可获得敏感信息，使应用程序崩溃或执行任意代码。

CNVD 收录的相关漏洞包括：Apple Safari 拖动文件信息泄露漏洞、Apple Safari 拖放跨域漏洞、Apple Safari URL 伪造漏洞、Apple Safari 访问控制漏洞、Apple Safari 拖放文件发送漏洞、Apple Safari 沙盒绕过漏洞、Apple Safari CSS 处理跨域漏洞、Apple Safari WebKit 内存破坏漏洞（CNVD-2012-13263）等。其中，“Apple Safari WebKit 内存破坏漏洞（CNVD-2012-13263）”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=52455
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=52400
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=52438
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=52375
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=52403
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=52476
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=52406
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=52435

2、Oracle 产品安全漏洞

Oracle Database Server 是一款数据库管理系统；Oracle E-Business Suite 是一款由 Oracle 公司推出的新一代电子商务套件。Oracle Fusion Middleware 是一款融合中间软件的产品；MySQL 是一个小型关系型数据库管理系统；PeopleSoft 是一款集成多个商务功能的企业软件；Oracle Siebel CRM 是一款客户关系管理解决方案。本周，上述产品被披露存在多个安全漏洞，攻击者可利用上述漏洞可获取敏感信息，发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Oracle Database Server Core RDBMS 组件远程拒绝服务漏洞、Oracle Database Server Network Layer 组件远程网络层拒绝服务漏洞、Oracle E-Business Suite 'Document Repository'子组件远程部分控制漏洞、Oracle E-Business Suite 远程部分控制漏洞、Oracle Fusion Middlewar 组件 JRockit 子组件远程漏洞（CNVD-2012-13137）、Oracle MySQL Server GIS Extension 子组件拒绝服务漏洞、Oracle PeopleSoft Enterprise PeopleTools 'CM'子组件远程信息泄露漏洞、Oracle Siebel CRM 'Portal Framework'子组件远程漏洞等。其中，“Oracle Fusion Middlewar 组件 JRockit 子组件远程漏洞（CNVD-2012-13137）”的综合评价为“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=52144
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=52143
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=52186
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=52188
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=52141

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=52169

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=52162

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=52171

3、ISC 产品安全漏洞

ISC DHCP 是一款开源的 DHCP 服务软件；ISC BIND 是一款 DNS 解析服务软件。本周，上述产品被披露存在多个安全漏洞，攻击者利用漏洞可消耗服务器大量内存，发送恶意报文，触发缓冲区溢出，使服务程序崩溃。

CNVD 收录的相关漏洞包括：ISC DHCP 内存泄露漏洞、ISC BIND 9 TCP 查询远程拒绝服务漏洞、ISC DHCP Server DHCPv6 拒绝服务漏洞、ISC DHCP 拒绝服务漏洞、ISC BIND 9 DNSSEC 校验远程拒绝服务漏洞。其中，“ISC BIND 9 DNSSEC 校验远程拒绝服务漏洞”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=52288

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=52283

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=52286

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=52284

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=52282

4、Symantec 产品安全漏洞

Symantec System Recovery 是一款系统备份和恢复解决方案，用于防止业务中断；Symantec Web Gateway 是一款 Web 安全网关硬件设备。本周，该产品被披露存在多个漏洞，远程攻击者可以利用漏洞提交恶意请求、注入任意代码并执行，获取数据库信息或控制应用系统。

CNVD 收录的相关漏洞包括：Symantec System Recovery DLL 装载任意代码执行漏洞、Symantec Web Gateway SQL 盲注漏洞、Symantec Web Gateway SQL 注入漏洞、Symantec Web Gateway shell 命令执行漏洞、Symantec Web Gateway 本地文件操作验证绕过漏洞、Symantec Web Gateway 代码注入漏洞、Symantec Web Gateway 密码更改安全绕过漏洞。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=52191

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=52198

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=52197

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=52193

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=52195

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=52194

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=52199

5、httpdx 通配符拒绝服务漏洞

httpdx 是一款轻型的 http 和 ftp 服务软件。本周，httpdx 被披露存在一个拒绝服务漏洞。远程攻击者可以利用漏洞提交恶意 GET 请求，使应用程序崩溃。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=52228

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-2012-13237	ASP-DEv XM Forums RC3 SQL 注入漏洞	高	暂无
CNVD-2012-13250	ZABBIX 'itemid'参数 SQL 注入漏洞	高	ZABBIX 2.0.2rc2 已经修复此漏洞，建议用户下载使用： https://support.zabbix.com/browse/ZBX-5348
CNVD-2012-13248	SquidClamav URL 解析拒绝服务漏洞	高	暂无
CNVD-2012-13232	WordPress 插件 Flexi Quote Rotator SQL 注入漏洞	高	用户可联系供应商获得补丁信息： http://wordpress.org/extend/plugins/flexi-quote-rotator/
CNVD-2012-13230	Wireshark PPP 拒绝服务漏洞	高	暂无
CNVD-2012-13221	Caucho Quercus Running On Resin 空字节注入漏洞	高	Caucho's Quercus on Resin 4.0.29 已经修复此漏洞，建议用户下载使用： http://caucho.com/products/ 无
CNVD-2012-13228	Siemens SIMATIC 产品 DLL 加载任意代码执行漏洞	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.siemens.com/corporate-technology/pool/de/forschungsfelder/siemens_security_advisory_ssa-110665.pdf
CNVD-2012-13207	Ipswitch WhatsUp Gold 'sGroupList'参数 SQL 注入漏洞	高	暂无
CNVD-2012-13199	AFD 缓冲区溢出漏洞（CNVD-2012-13199）	高	目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载： http://www.dwd.de

CNVD-2012-13202	Dell SonicWALL Scrutinizer 'q'参数 SQL 注入漏洞	高	Dell SonicWALL Scrutinizer 9.5.2 已经修复此漏洞，建议用户下载使用： http://www.mysonicwall.com
CNVD-2012-13328	PHPCMS v9 文件包含漏洞	中	暂无

表 3 部分高危漏洞列表

小结：本周，Oracle 的多款产品以及 Apple Safari 浏览器被披露存在多个漏洞，攻击者利用漏洞使应用程序崩溃，发起拒绝服务攻击。ISC 的两款产品被披露存在的漏洞可消耗服务器大量内存，攻击者可利用漏洞发送恶意报文，使服务程序崩溃。Symantec 产品存在的漏洞可提交恶意请求注入任意代码并执行，获取数据库信息或控制应用系统。此外，httpdx 服务软件和国内厂商生产的网站内容管理系统软件 PHPCMS 被披露存在零日漏洞，对相关网络服务器安全构成威胁，需着重加强防范。

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 MQ 和 InfoSphere Identity Insight 安全漏洞

IBM WebSphere MQ 是一款用于在企业中提供消息传输服务的解决方案；IBM InfoSphere Identity Insight 是一个分析平台，用于应对网络欺诈。本周，IBM 发布升级程序，修补了 WebSphere MQ 和 InfoSphere Identity Insight 存在的漏洞。攻击者可以利用漏洞访问队列管理器或提升权限。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=19152
http://www.cnvd.org.cn/sites/main/preview/bdgg_preview.htm?tid=19234

本周要闻速递

1. 乌云称 MIUI 漏洞导致小米用户短信等隐私泄露

7 月 27 日，乌云漏洞报告平台曝光小米手机 MIUI 系统存在漏洞，可造成用户大量敏感数据泄露。由于 MIUI 备份数据明文存储在 SD 卡中，攻击者可利用漏洞获取小米手机用户的联系人列表、短信内容、WIFI 密码以及本地应用程序的私有数据等。漏洞信息显示，MIUI 用户使用备份程序(Backup.apk)所生成的备份信息被自动保存在 SD 卡中，而 Android 的系统加密机制仅针对手机内存中的文件有效，并不对 SD 卡的文件读写进行权限加密；同时，MIUI 也未对备份信息进行加密，从而使任意手机程序都可以读取这些明文保存的备份信息。MIUI 的备份信息中不仅包含手机用户的联系人、短信

内容等信息，还有用户所安装软件的详细信息，攻击者一旦使用伪装过的恶意软件 APK 文件替换掉备份数据中的正常文件，那么用户在进行系统恢复后，恶意软件便会被恢复至系统中，黑客可借此持续窃取 MIUI 用户信息。此外，该漏洞还可将 MIUI 用户已安装软件中的隐私数据从手机内存的私有目录拷贝至 SD 卡，没有了手机内存的加密机制，不仅联系人、短信内容等信息无法被保护，诸如微博、SNS 等软件中的个人信息也会被黑客窃取。据了解，该漏洞于 6 月 11 日就被曝出，影响所有 MIUI 版本，此后小米公司也已确认该漏洞，但并未透露将于何时推出补丁。

参考链接：<http://digi.hsw.cn/system/2012/07/27/051399360.shtml>

2. Facebook 斥资 40 万美元招募黑客查找安全漏洞

北京时间 7 月 29 日消息，据国外科技博客网站 The Verge 报道，在本周于拉斯维加斯举行的 DefCon 国际黑客大会上，Facebook 不仅新招募了一些安全专家，同时欢迎黑客在 Facebook 上查找安全漏洞，并对于发现者给予资金奖励。据悉，Facebook 此前面向黑客推出了一项名为“bug bounties”的服务，该服务鼓励全球黑客从 Facebook 产品上找出漏洞，并给予奖励。而此次 Facebook 的奖励范围扩大到了 Facebook 的服务器和基础设施领域。为此 Facebook 已准备好了高达 40 万美元的奖金。Facebook 会根据所发现 BUG 的重要性，对黑客进行 500 美元至 10000 美元的奖励。而对于黑客发现与 Facebook 有关的：拒绝式攻击、垃圾技术、第三方应用漏洞以及第三方站点漏洞等，Facebook 一律不予奖励。

参考链接：http://news.itxinwen.com/it_industry/business_software/2012/0730/430346.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