

信息安全漏洞周报

2012 年 6 月 25 日-2012 年 7 月 1 日

2012 年第 26 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 134 个，其中高危漏洞 61 个、中危漏洞 62 个、低危漏洞 11 个。上述漏洞中，可利用来实施远程攻击的漏洞有 126 个。本周收录的漏洞中，已有 95 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“VLC Media Player '.avi'拒绝服务漏洞”、“Real Networks RealPlayer '.avi'除零拒绝服务漏洞”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 134 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，上海交通大学向 CNVD 提交了 4 个原创漏洞。

报送单位或个人	漏洞报送数量	原创漏洞数量
绿盟科技	115	0
启明星辰	87	0
安天实验室	30	0
天融信	21	0
恒安嘉新	14	0
东软	3	0
安氏领信	9	0
上海交通大学	4	4
报送总计	283	4
总计	134（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 Google、Oracle、IBM、Cisco、WordPress 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	22	16%
2	Oracle	10	7%
3	IBM	8	6%
4	WordPress	7	5%
5	Cisco	7	5%
6	HP	6	4%
7	Symantec	4	3%
8	Eaton MGE Office Protection Systems	3	2%
9	DMS-Easy	3	2%
10	Squiz	2	1%
11	其它	62	49%

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 134 个漏洞。其中操作系统漏洞 2 个，应用程序漏洞 97 个，WEB 应用漏洞 30 个，数据库漏洞 1 个，网络设备漏洞 4 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	97
WEB 应用漏洞	30
网络设备漏洞	4
数据库漏洞	1
安全产品漏洞	0

表 3 漏洞按影响类型统计表

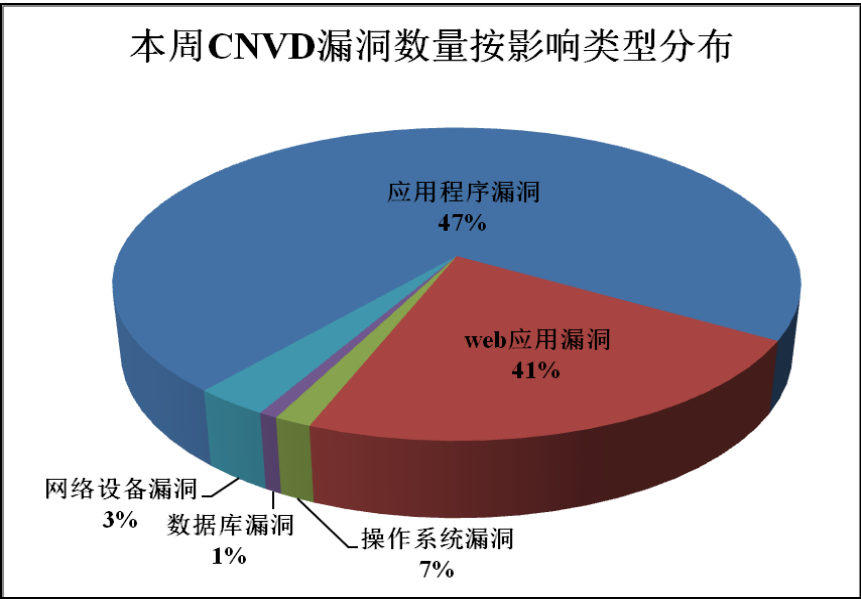


图 1 本周漏洞按影响类型分布

本周涉及电信行业漏洞信息

本周，CNVD 收录了 4 个网络设备漏洞，其中，“Cisco AnyConnect Secure Mobility Client VPN Downloader 任意代码执行漏洞（CNVD-2012-12683）”和“Cisco AnyConnect Secure Mobility Client VPN Downloader 任意代码执行漏洞（CNVD-2012-12685）”的综合评级为“高危”，“ASUS iKVM 信息泄露漏洞”和“HP Photosmart Printers 拒绝服务漏洞”的综合评级均为“中危”。

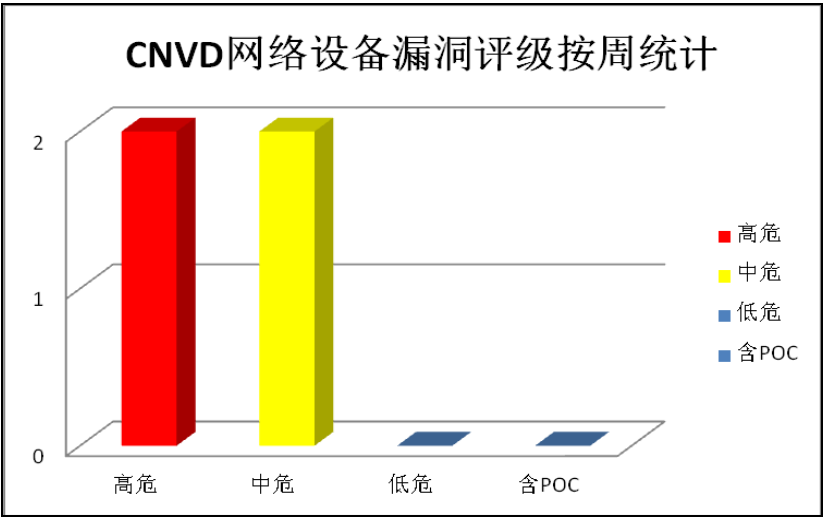


图 2 网络设备漏洞统计

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、Google Chrome 安全漏洞

Google Chrome 是一款开源的 WEB 浏览器。本周，该产品被披露存在多个安全漏洞，攻击者利用漏洞可提升权限，使应用程序崩溃，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 安全绕过漏洞（CNVD-2012-12716）、Google Chrome 节表内存错误引用漏洞、Google Chrome counter layout 内存错误引用漏洞、Google Chrome SVG 资源处理漏洞、Google Chrome Mac UI 内存错误引用漏洞、Google Chrome 不正确 DLL 装载漏洞、Google Chrome PDF JS API 缓冲区溢出漏洞、Google Chrome libxml 整数溢出漏洞等。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=51040
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=51041
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=51042
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=51051
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=51057
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=51063
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=51069
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=51074

2、HP 产品安全漏洞

HP System Management Homepage 是一款 HP 公司发布的系统管理软件。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提升权限，获得敏感信息，发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：HP System Management Homepage 输入验证漏洞、HP System Management Homepage 特权提升漏洞、HP System Management Homepage 信息泄露漏洞、HP System Management Homepage 拒绝服务漏洞、HP System Management Homepage AUTOCOMplete 启用漏洞。其中，“HP System Management Homepage AUTOCOMplete 启用漏洞”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=51064
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=51066
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=51067
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=51062
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=51058

3、IBM 产品安全漏洞

IBM AIX 是一款商业主机操作系统；IBM Rational Directory Server 是一款目录服务程序；IBM Lotus Expeditor 是 IBM 的通用受管客户机软件。本周，上述产品被披露存在多个安全漏洞，攻击者利用漏洞可重定向用户通信，读取系统上任意文件信息，以 root 特权执行任意代码。

CNVD 收录的相关漏洞包括：IBM AIX Sendmail 本地权限提升漏洞、IBM Rational Directory Server 帮助系统跨站脚本漏洞、IBM Rational Directory Server 帮助系统重定向漏洞、IBM Lotus Expeditor DLL 装载任意代码执行漏洞、IBM Lotus Expeditor 'Eclipse Help'组件目录遍历漏洞、IBM Lotus Expeditor 请求头伪造安全绕过漏洞。其中，“IBM Lotus Expeditor DLL 装载任意代码执行漏洞”和“IBM AIX Sendmail 本地权限提升漏洞”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=51070
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=50937
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=50935
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=50932
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=50933
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=50934

4、Oracle 产品安全漏洞

Sun Java Runtime Environment 是一款为 JAVA 应用程序提供可靠运行环境的解决方案。本周，该产品被披露存在多个漏洞。攻击者利用漏洞可获取敏感信息，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 SE Hotspot 子组件任意代码执行漏洞（CNVD-2012-12678）、Oracle Java Runtime Environment 组件 Networking 子组件存在未明漏洞、Oracle Java SE Deployment 子组件任意代码执行漏洞（CNVD-2012-12674）、Oracle Java SE Deployment 子组件任意代码执行漏洞（CNVD-2012-12672）、Oracle Java Runtime Environment 组件 JAXP 子组件拒绝服务漏洞、Oracle Java Runtime Environment 组件 Libraries 子组件存在未明漏洞、Oracle Java Runtime Environment 组件存在未明漏洞、Oracle Java Runtime Environment 组件 CORBA 子组件部分控制漏洞等。

其中，“Oracle Java Runtime Environment 组件存在未明漏洞”、“Oracle Java SE Deployment 子组件任意代码执行漏洞（CNVD-2012-12672）”、“Oracle Java SE Deployment 子组件任意代码执行漏洞（CNVD-2012-12674）”、“Oracle Java SE Hotspot 子组件任意代码执行漏洞（CNVD-2012-12678）”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=50982
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=50975

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=50978
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=50976
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=50981
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=50984
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=50955
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=50956

5、VLC Media Player '.avi'拒绝服务漏洞

VLC Media Player 是一款多媒体播放程序。本周，VLC Media Player 被披露存在一个综合评级为“高危”的拒绝服务漏洞。攻击者可以利用漏洞构建恶意文件，诱使用户解析，触发除零错误导致应用程序崩溃。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=51108

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-2012-12748	SAP Netweaver ABAP 'msg_server.exe'远程代码执行漏洞	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.sdn.sap.com/irj/sdn/index?rid=/webcontent/uuid/c05604f6-4eb3-2d10-eea7-ceb666083a6a#section40
CNVD-2012-12712	WordPress 插件 Website FAQ 'category' SQL 注入漏洞	高	暂无
CNVD-2012-12711	Kingview 网络缓冲区溢出漏洞	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.kingview.com
CNVD-2012-12693	Cotonti 'admin.php' SQL 注入漏洞	高	暂无
CNVD-2012-12752	GE Proficy 产品栈缓冲区溢出漏洞	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://support.ge-ip.com/support/index?page=kbchannel
CNVD-2012-12670	Amazon S3 Uploadify 脚本 'uploadify.php'脚本任意文件上传漏洞	高	暂无

CNVD-2012-12710	Support Tickets MyTickets 'MyTickets_language' SQL 注入漏洞	高	Support Tickets MyTickets 2.0.9 版本已修复此漏洞，建议用户下载使用： http://phpx3.com/scripts.html#mytickets
CNVD-2012-12703	Symantec Message Filter 会话固定漏洞（CNVD-2012-12703）	高	暂无
CNVD-2012-12673	Apache Roller 跨站请求伪造漏洞	高	Apache Roller 5.0.1 已经修复此漏洞，建议用户下载使用： http://roller.apache.org/
CNVD-2012-12684	SugarCRM Community Edition 'unserialize()' PHP 代码执行漏洞	高	SugarCRM Community Edition 6.4.0 已经修复此漏洞，建议用户下载使用： http://www.sugarcrm.com/

表 3 部分高危漏洞列表

小结：本周，Google Chrome、HP System Management Homepage、Sun Java Runtime Environment 以及 IBM 的多款产品被披露存在多个漏洞，攻击者利用漏洞可提升权限，获取系统敏感信息，发起拒绝服务攻击或执行任意代码。此外，VLC Media Player 播放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、Linux 发布升级程序，修补 kernel 安全漏洞

Linux Kernel 是开源操作系统 Linux 所使用的内核。本周，Linux 发布升级程序，修补了 Kernel 存在的漏洞。远程攻击者可利用漏洞发起拒绝服务或栈缓冲区溢出攻击。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=18432

本周要闻速递

1. MySQL 数据库各版本曝出重大漏洞

据悉，MySQL 几乎所有版本爆出了重大漏洞，将允许不知道密码只知道用户名的用户登录进入 MySQL。TechTarget 数据库网站编辑随即查看了漏洞的具体信息，在 MySQL 和 MariaDB 数据库服务器的更新漏洞补丁 CVE-2012-2122 中，假定了 memcmp（）函数的返回值是在-127 到 127 范围内。然而在启用某些优化机制的平台上，程序的返回值将超出规定的范围，这将导致在输入错误用户密码的情况下返回 true 值，使得在没有密码的用户将有机会登录到数据库服务器。

参考链接: <http://www.ciotimes.com/infrastructure/sjk/66433.html>

2. 谷歌 Chrome 漏洞导致新款 MBA 崩溃

本月 WWDC 大会上苹果发布新款 MacBook Air 后就有用户反应他们的设备经常遭遇崩溃问题。Gizmodo 此前指出这个问题是因为谷歌的 Chrome 浏览器导致的, 如果用户更换使用苹果的 Safari 浏览器崩溃问题便可解决。目前谷歌已经发表正式声明, 承认 Chrome 导致设备崩溃, 确定 Chrome 浏览器中的图形资源所存在的漏洞, 它与 Mac OS X 上的绘图插件相关。这个资源漏洞会让使用 Intel HD 4000 新卡的 Mac 硬件 (比如新款 MacBook Air) 出现内核错误。根据谷歌发布的声明, 所有使用 Intel HD 4000 显卡的系统均受到这个问题的影响, 也就是谁苹果本月初发布的新款笔记本均易出现该问题, 据悉部分新款 MBP 机型的用户也反应他们的设备会因为 Chrome 而崩溃。

参考链接: http://tech.ifeng.com/apple/news/detail_2012_06/29/15667333_0.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