

信息安全漏洞周报

2012 年 5 月 14 日-2012 年 5 月 20 日

2012 年第 20 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 145 个，其中高危漏洞 54 个、中危漏洞 87 个、低危漏洞 4 个。上述漏洞中，可利用来实施远程攻击的漏洞有 138 个。本周收录的漏洞中，已有 91 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“Viscacha CMS SQL 注入漏洞”、“Travelon Express 'hid' SQL 注入漏洞”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 145 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、恒安嘉新、安天实验室等单位报送数量较多。此外，上海交通大学以及多位个人漏洞研究者向 CNVD 提交了 16 个原创漏洞，其中涉及多个国内工业控制系统漏洞案例。

报送单位或个人	漏洞报送数量	原创漏洞数量
绿盟科技	87	0
启明星辰	108	0
恒安嘉新	36	0
安天实验室	27	0
安氏领信	2	0
东软	22	0
上海交通大学	5	5
个人上报者	11	11
报送总计	298	16

总计	145（去重）	16
----	---------	----

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Microsoft、WordPress 、Apple、Emerson Electric Co. 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	20	13.8%
2	WordPress	18	12.4%
3	Apple	11	7.6%
4	Emerson Electric Co.	5	3.4%
5	SAP	4	2.8%
6	RealPlayer	3	2.0%
7	Hitachi	3	2.0%
8	Symantec	3	2.0%
9	Ubuntu	2	1.4%
10	Adobe	2	1.4%
11	其它	74	51.2%

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 145 个漏洞。其中操作系统漏洞 5 个，应用程序漏洞 89 个，WEB 应用漏洞 45 个，安全产品漏洞 1 个，网络设备漏洞 5 个。

漏洞影响对象类型	漏洞数量
操作系统漏洞	5
应用程序漏洞	89
WEB 应用漏洞	45
网络设备漏洞	5
数据库漏洞	0
安全产品漏洞	1

表 3 漏洞按影响类型统计表

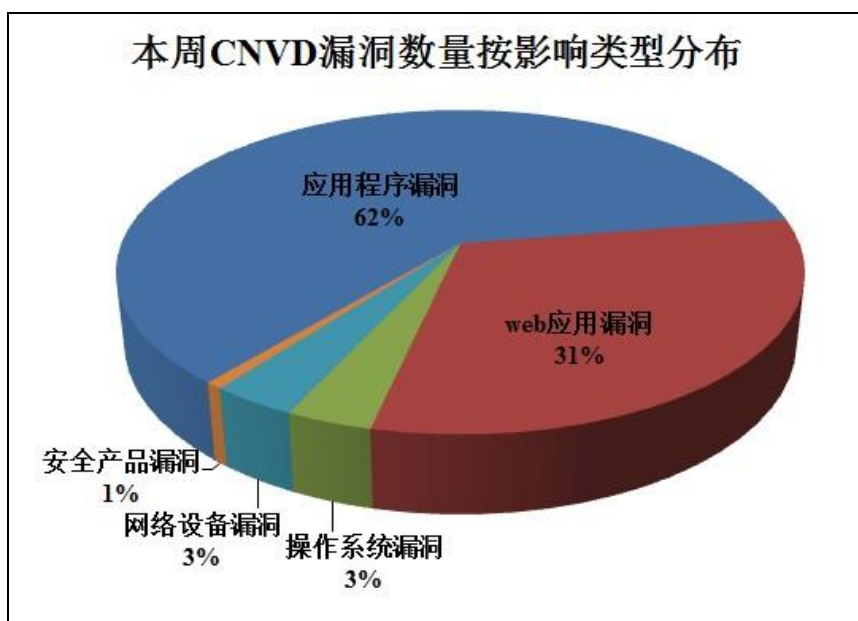


图 1 本周漏洞按影响类型分布

本周涉及电信行业漏洞信息

本周，CNVD 收录了 5 个网络设备漏洞，其中，“Symantec Web Gateway 远程 shell 命令执行漏洞”、“Symantec Web Gateway Management 脚本任意文件上传漏洞”的综合评级为“高危”。“Symantec Web Gateway Management 任意文件下载删除漏洞”、“Belkin N150 Wireless Router 'login.stm'管理员密码信息泄露漏洞”和“NETGEAR WND RMAC Wireless Router 存在多个信息泄露漏洞”的综合评级为“中危”。目前，互联网上已经出现针对“Belkin N150 Wireless Router 'login.stm'管理员密码信息泄露漏洞”的攻击代码。

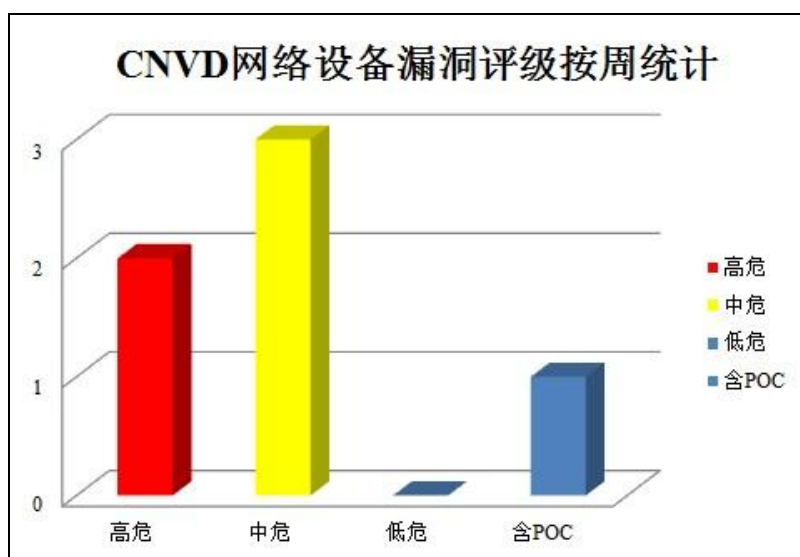


图 2 网络设备漏洞统计



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，Google Chrome 被披露存在多个安全漏洞，攻击者可以利用漏洞执行指定代码，导致应用程序崩溃。CNVD 收录的相关漏洞包括：Google Chrome libxml 单字节越界写漏洞、Google Chrome 装载链接漏洞、Google Chrome Windows Media Player 插件漏洞、Google Chrome 样式元素内存错误引用漏洞、Google Chrome 窗口导航漏洞、Google Chrome worker 竞争条件漏洞、Google Chrome 表单处理内存错误引用漏洞、Google Chrome indexed DB 内存错误引用漏洞等。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=49035
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=49007
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=49028
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=49010
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=49012
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=49017
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=49015
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=49018

2、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 被披露存在多个安全漏洞，攻击者可以利用漏洞窃取 Cookie 身份凭据，执行任意 HTML 和相关脚本代码。CNVD 收录的相关漏洞包括：WordPress 插件 Sharebar SQL 注入漏洞、WordPress 插件 Download Monitor 'uploader.php'存在多个跨站脚本漏洞、WordPress 插件 Dynamic Widgets 'themes.php' 跨站脚本漏洞、WordPress 插件 iFrame Admin Pages 'main_page.php'跨站脚本漏洞、WordPress 插件 Network Publisher 'networkpub_key'跨站脚本漏洞、WordPress 插件 Sharebar 跨站脚本漏洞、WordPress WP Forum Server 'groupid'跨站脚本漏洞、WordPress 插件 Media Library Categories 'q'跨站脚本漏洞等。其中，“WordPress 插件 Sharebar SQL 注入漏洞”的综合评级为“高危”。目前，厂商已经发布了“WordPress 插件 Download Monitor 'uploader.php'存在多个跨站脚本漏洞”和“WordPress 插件 Network Publisher 'networkpub_key'跨站脚本漏洞”的补丁。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=48955
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=49050

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=49049

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=49048

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=48926

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=48956

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=48934

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=48930

3、Symantec 产品安全漏洞

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安全漏洞，攻击者可以利用漏洞下载和删除任意文件，向应用程序脚本注入任意代码，并以应用程序权限执行。CNVD 收录的相关漏洞包括：Symantec Web Gateway Management 任意文件下载删除漏洞、Symantec Web Gateway Management 脚本任意文件上传漏洞、Symantec Web Gateway 远程 shell 命令执行漏洞。其中，“Symantec Web Gateway Management 脚本任意文件上传漏洞”和“Symantec Web Gateway 远程 shell 命令执行漏洞”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=49080

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=49078

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=49083

4、Apple 产品安全漏洞

Apple Mac OS X 是一款苹果公司开发的操作系统；Apple QuickTime 是一款多媒体播放器。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构建恶意文件，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 QuickTime .pict 内存破坏漏洞、Apple QuickTime 文件路径缓冲区溢出漏洞、Apple QuickTime Sorenson 编码文件任意代码执行漏洞、Apple Mac OS X QuickTime 内存错误引用漏洞、Apple Mac OS X QuickTime MPEG 处理缓冲区溢出漏洞、Apple Mac OS X QuickTime MPEG 处理整数溢出漏洞、Apple Mac OS X QuickTime 缓冲区溢出漏洞、Apple Mac OS X X.509 证书处理任意代码执行漏洞等。其中，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=49006

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=49008

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=49002

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=48737

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=48736

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=48735

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=48751

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=48746

5、Travelon Express 'hid' SQL 注入漏洞

Travelon Xpress 是一款内容管理系统。本周，Travelon Xpres 被披露存在一个综合评级为“高危”的 SQL 注入漏洞，主要影响 6.2 版本。由于 holiday.php 和 holiday_book.php 中“hid”参数未能正确过滤，攻击者可以利用漏洞发起 SQL 注入攻击，获得后台数据库信息。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=48879

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-2012-11967	DeltaV 多个产品文件操作漏洞	高	暂无
CNVD-2012-11954	libxml2 'xmlXPathEvalXPathPart()' 函数单字节缓冲区溢出漏洞	高	供应商发布了相关补丁信息，修复了此漏洞，建议用户下载使用。避免攻击者构建恶意数据，诱使应用程序解析，可触发越界写错误： http://git.gnome.org/browse/libxml2/commit/?id=d8e1faea99c7a7c07af01c1c72de352eb590a3e
CNVD-2012-11968	Epicor Returns Management SOAP 接口 SQL 注入漏洞	高	供应商发布了相关补丁信息，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可获得数据库信息或控制应用系统： http://www.epicor.com/Pages/default.aspx
CNVD-2012-11931	ispVM System '.xcf'文件缓冲区溢出漏洞	高	暂无
CNVD-2012-11944	RealPlayer RealMedia RealJukebox Media 解析器缓冲区溢出漏洞	高	供应商发布了相关补丁信息，修复了此漏洞，建议用户下载使用： http://www.apple.com/quicktime/
CNVD-2012-11876	gdk-pixbuf 'read_bitmap_file_data()'整数溢出漏洞	高	供应商发布了相关补丁信息，修复了此漏洞，建议用户下载使用。避免攻击者通过特制的 XBM 文件可导致基于堆的缓冲区溢出： https://bugs.launchpad.net/ubuntu/source/gdk-pixbuf/bug/681150

CNVD-2012-11933	Lattice Diamond 存在多个内存破坏漏洞	高	暂无
CNVD-2012-11844	Galette 'id_adh' SQL 注入漏洞	高	供应商发布了相关补丁信息，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通过注入任意 SQL 代码操作 SQL 查询： http://galette.tuxfamily.org/dc/index.php/
CNVD-2012-11929	ispLEVER Classic 项目文件处理缓冲区溢出漏洞	高	暂无
CNVD-2012-11924	HP Business Service Management 远程代码执行漏洞 (CNVD-2012-11924)	高	暂无

表 3 部分高危漏洞列表

小结：本周，Google Chrome 浏览器以及 Apple 的多款产品被披露存在漏洞，攻击者可以利用漏洞构建恶意文件，使应用程序崩溃或执行任意代码。网关设备 Symantec Web Gateway 以及网站内容管理系统 WordPress 被披露存在多个漏洞，攻击者可以利用漏洞窃取敏感信息或执行任意代码。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。此外，Travelon Express 还被披露存在零日漏洞。

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、Adobe 发布升级程序，修补 Photoshop 安全漏洞

本周，Adobe 发布升级程序，修补了 Photoshop 两个综合评级为“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。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=16973

本周要闻速递

1. 微软公司发布 5 月份漏洞补丁

微软公司发布了 5 月份的漏洞补丁程序，修复了存在的多个漏洞。其中，MS12-034: Microsoft .NET Framework 序列化远程代码执行漏洞，危害等级为“严重”。Microsoft .NET Framework 中存在一个远程执行代码漏洞，它可能允许特制的 Microsoft .NET Framework 应用程序以不安全的方式访问内存。成功利用此漏洞的攻击者可以在登录

用户的安全上下文中运行任意代码。攻击者可随后安装程序；查看、更改或删除数据。

参考链接：<http://security.ctocio.com.cn/412/12336912.shtml>

2. 谷歌 Chrome19 更新修复 20 个高危漏洞

据报道，Chrome 19 修复的 20 个安全漏洞中，其中 7 个漏洞被 Google 简报称为“出乎意料”的读写缺陷，还有 11 个漏洞是由 Google 的安全小组或委托微软找出的。而且因为有 6 个研究者报告出了 9 个漏洞，Google 奖励了他们 7500 美金。此前，Google 也为好几个研究者发了 9000 美元奖励，其中一些研究者在 Chrome 19 开发过程中就指出了存在的漏洞。据报道，在之前版本中，Chrome 就已经支持对书签、应用、扩展、历史、主题和设置的同步。这次它的最大的变化在于增加了对已打开标签的同步支持。同时，Chrome 19 将支持多平台操作，包括 Android。

参考链接：http://news.ccidnet.com/art/11099/20120517/3862421_1.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