

信息安全漏洞周报

2012 年 3 月 19 日-2012 年 3 月 25 日

2012 年第 12 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 160 个，其中高危漏洞 45 个、中危漏洞 115 个、低危漏洞 0 个。上述漏洞中，可利用来实施远程攻击的漏洞有 153 个。本周收录的漏洞中，已有 73 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“Dell Webcam 'crazytalk4.ocx' ActiveX 缓冲区溢出漏洞”、“TYPSoft FTP Server 'APPE'命令远程缓冲区溢出漏洞”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 7 家成员单位报送了本周收录的全部 160 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、天融信等单位报送数量较多。此外，接收到成员单位恒安嘉新报送了国产某办公 OA 软件系统存在的多个跨站漏洞。国内漏洞研究者（个人报送者）向 CNVD 报送了 3 起涉及政府和重要信息系统部门的漏洞事件。

报送单位或个人	漏洞报送数量	原创漏洞数量
启明星辰	145	0
绿盟科技	97	0
安天实验室	29	0
天融信	22	0
恒安嘉新	6	1
东软	4	0
安氏领信	4	0
个人上报者	3	3
报送总计	310	4

总计	160（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、Moodle、VMware、RSA Security、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	Google	9	5.6%
2	Moodle	9	5.6%
3	VMware	7	4.3%
4	RSA Security	5	3.1%
5	Linux	5	3.1%
6	Apache Software Foundation	3	1.9%
7	Novell	2	1.2%
8	Quantum	2	1.2%
9	Microsoft	2	1.2%
10	Asterisk	2	1.2%
11	其它	114	71.6%

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 160 个漏洞。其中操作系统漏洞 3 个，应用程序漏洞 89 个，WEB 应用漏洞 18 个，数据库漏洞 0 个，网络设备漏洞 5 个，安全产品漏洞 45 个。

漏洞影响对象类型	漏洞数量
操作系统漏洞	3
应用程序漏洞	89
WEB 应用漏洞	18
数据库漏洞	0
网络设备漏洞	5
安全产品漏洞	45

表 3 漏洞按影响类型统计表

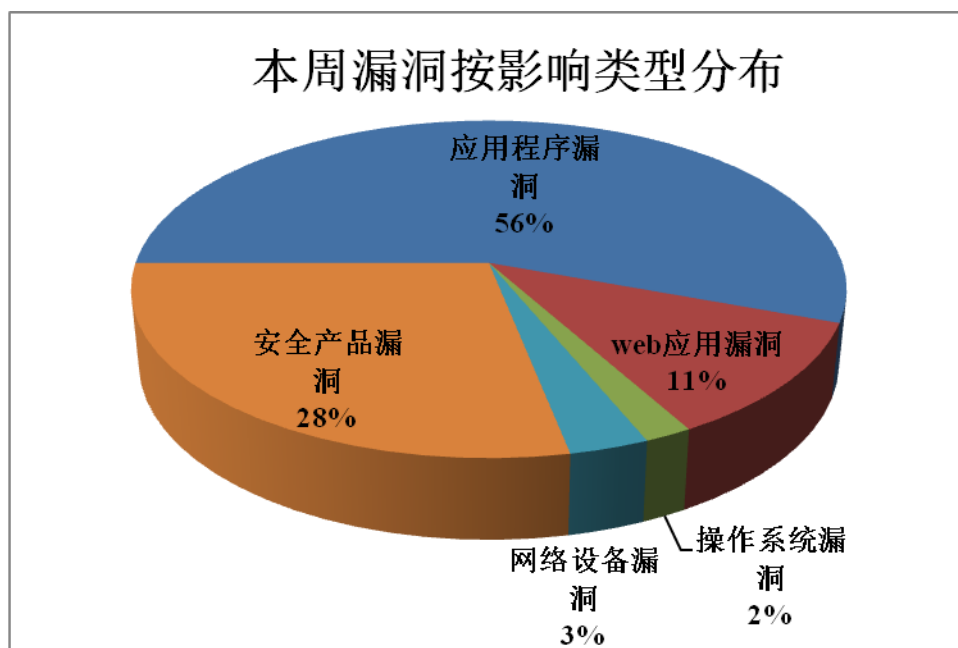


图 1 本周漏洞按影响类型分布

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“Cisco Wireless-G PTZ Internet Video Camera WVC200 'PlayerPT.ocx'缓冲区溢出漏洞”的综合评级为“高危”。 “LG-Nortel ELO GS24M 交换机验证凭据信息泄露漏洞”、“LG-Nortel ELO GS24M 交换机验证凭据验证绕过漏洞”、“Quantum Scalar i500, Dell ML6000 和 IBM TS3310 企业磁带库 WEB 接口跨站脚本漏洞”、“Quantum Scalar i500, Dell ML6000 和 IBM TS3310 磁带库预配置密码漏洞”的综合评级为“中危”。目前，互联网上已经出现针对“Cisco Wireless-G PTZ Internet Video Camera WVC200 'PlayerPT.ocx'缓冲区溢出漏洞”的攻击代码。

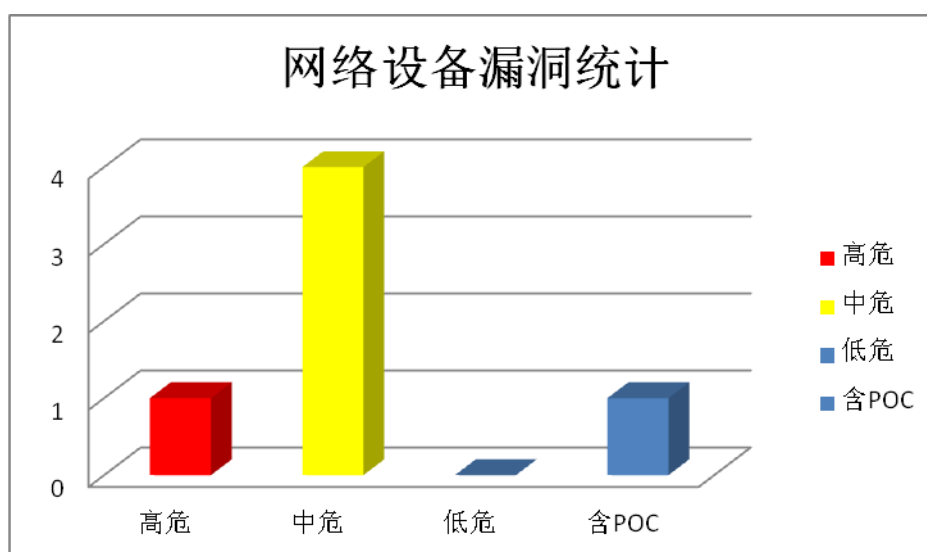


图 2 网络设备漏洞统计

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、Apache 产品安全漏洞

Apache Wicket 是基于组件的轻量级 Web 应用框架；mod_fcgid 是一个跟 mod_fastcgi 兼容的 Apache 模块组件。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窃取敏感信息、在目标用户浏览器上执行恶意脚本代码或发起拒绝服务攻击。CNVD 收录的相关漏洞包括：Apache Wicket 'pageMapName'参数跨站脚本漏洞、Apache Wicket 隐藏文件信息泄露漏洞、Apache 'mod_fcgid'模块拒绝服务漏洞。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=45275
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=45276
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=44919

2、Google Chrome 安全漏洞

Google Chrome 是一款 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绕过安全限制、执行任意代码或造成拒绝服务。CNVD 收录的相关漏洞包括：Google Chrome WebUI 特权存在漏洞、Google Chrome 非法读漏洞、Google Chrome 跨越策略存在漏洞、Google Chrome 内存错误引用漏洞（CNVD-2012-10800、CNVD-2012-10803、CNVD-2012-10801）、Google Chrome 远程代码执行漏洞、Google Chrome 解压扩展存在漏洞。上述漏洞的综合评级均为“高危”。目前，Google 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=44415
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=45339
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=45337
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=45335
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=45320
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=45342
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=45356
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=45341

3、VMware 产品安全漏洞

VMware View Manager 是一款企业级虚拟桌面管理器；VMware vCenter Orchestrator 为 VMware vCenter 任务创建自动化工作流；VMware vSphere Client 是 Windows 程序，可用于配置主机和运行主机之上的虚拟机。本周，上述 VMware 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 URL 诱使用户解析，获得敏感信息或劫

持用户会话，触发缓冲区溢出提升特权。CNVD 收录的相关漏洞包括：VMware vCenter Orchestrator 密码泄露漏洞、VMware View Manager Portal 跨站脚本漏洞、VMware View 特权提升漏洞（CNVD-2012-10685、CNVD-2012-10687、CNVD-2012-10686）、VMware vSphere 客户端日志项脚本注入漏洞、VMware vShield Manager 跨站脚本漏洞。其中，“VMware View 特权提升漏洞（CNVD-2012-10685、CNVD-2012-10687、CNVD-2012-10686）”的漏洞综合评级为“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=44575
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=44596
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=44576
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=44555
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=44578
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=44535
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=44536

4、多个安全产品存在漏洞

本周，PCTools、Sophos、CAT-QuickHeal 等多个反病毒软件厂商的产品被披露存在安全漏洞。攻击者可以利用漏洞构建恶意文件绕过相关安全产品的查杀检测。根据披露的情况，CNVD 重点收录了 Antivirus 相关漏洞，包括：多个 AntiVirus 产品 TAR 文件扫描绕过漏洞（CNVD-2012-10758）、多个 AntiVirus 产品 MS office 文件扫描绕过漏洞（CNVD-2012-10775）、多个 AntiVirus 产品 CAB 文件扫描绕过漏洞（CNVD-2012-10782）、Comodo AntiVirus MS EXE 文件扫描绕过漏洞（CNVD-2012-10744）、多个 AntiVirus 产品 ELF 文件扫描绕过漏洞（CNVD-2012-10761、CNVD-2012-10781、CNVD-2012-10779）、多个 AntiVirus 产品 ELF 文件扫描绕过漏洞（CNVD-2012-10764）。目前，厂商尚未发布上述漏洞的修补程序，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=45117
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=45220
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=45235
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=45015
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=45155
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=45226
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=45224
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=45158

5、Dell Webcam 'crazytalk4.ocx' ActiveX 缓冲区溢出漏洞

Dell Webcam 是一款网络摄像头软件。本周，Dell Webcam 绑定的 CrazyTalk4 ActiveX 控件被披露存在缓冲区溢出漏洞，允许攻击者构建恶意 WEB 页，诱使用户解析，

以应用程序上下文执行代码。当处理某些参数时, CrazyTalk4Native.dll 模块提供的 CrazyTalk4 ActiveX 控件存在边界错误, 向"BackImage", "ScriptName", "ModelName"和"SRC"等参数提交超长字符串可触发基于栈的溢出。目前, 互联网上已经出现针对该漏洞的攻击代码, 厂商尚未发布上述漏洞的修补程序, 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=44941

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-2012-10766	libzip 缓冲区溢出漏洞 (CNVD-2012-10766)	高	供应商发布了安全公告及相关补丁信息, 修复了此漏洞, 建议用户下载使用。避免被利用通过特制的 ZIP 文件引用已分配缓冲区之外的内存: http://nih.at/libzip/index.html
CNVD-2012-10712	WebGlimpse 'webglimpse.cgi'远程命令执行漏洞	高	供应商发布了安全公告及相关补丁信息, 修复了此漏洞, 建议用户下载使用。避免攻击者可以利用此漏洞执行任意命令安装 PHP 后门等: http://webglimpse.net/
CNVD-2012-10771	Novell ZENworks Configuration Management 存在多个漏洞	高	供应商发布了安全公告及相关补丁信息, 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获得敏感文件信息或执行任意代码: http://www.novell.com/products/zenworks/configurationmanagement/
CNVD-2012-10714	Adobe Photoshop '.tiff'文件内存错误引用漏洞	高	暂无
CNVD-2012-10739	InspIRCd 堆内存破坏漏洞	高	暂无
CNVD-2012-10710	Joomla! 'index.php' SQL 注入漏洞	高	供应商发布了安全公告及相关补丁信息, 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危及应用程序, 访问或修改数据, 或利用底层数据库中的潜在漏洞: http://www.joomla.org/
CNVD-2012-10706	VLC Media Player MMS 支持栈缓冲区溢出漏洞	高	供应商发布了安全公告及相关补丁信息, 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以应用程序上下文执行任意代码: http://www.videolan.org/

CNVD-2012-10736	FreePBX 远程命令执行漏洞	高	暂无
CNVD-2012-10678	Asterisk 缓冲区溢出漏洞	高	供应商发布了安全公告及相关补丁信息，修复了此漏洞，建议用户下载使用。避免利用漏洞可以以应用程序上下文执行任意代码： http://downloads.asterisk.org
CNVD-2012-10742	Dedecms 疑似被植入后门漏洞	高	暂无

表 3 部分高危漏洞列表

小结：本周，Google Chrome 被披露存在多个安全漏洞，攻击者可以利用漏洞绕过安全限制，执行任意代码或造成拒绝服务。多款安全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，绕过检测。此外，Apache 和 VMware 产品也被披露存在多个漏洞。Dell Webcam 零日漏洞也需引起相关用户注意，加强防范。

Dedecms 内容管理软件被披露存在一个疑似被植入后门漏洞。攻击者可利用此漏洞获得 WEB SHELL。CNVD 提醒使用上述软件的相关机构和个人及时采取安全防范措施。

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、RSA Security 发布升级程序，修补 enVision Platform 安全漏洞

本周，RSA Security 发布升级程序，修补了 enVision Platform 存在的安全漏洞。攻击者可以利用漏洞进行目录遍历攻击，以应用程序上下文查看系统文件内容，获得数据库信息或控制应用程序，甚至对系统进行未授权访问。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=14014

http://www.cnvd.org.cn/sites/main/preview/bdgg_preview.htm?tid=14011

http://www.cnvd.org.cn/sites/main/preview/bdgg_preview.htm?tid=13991

http://www.cnvd.org.cn/sites/main/preview/bdgg_preview.htm?tid=14013

http://www.cnvd.org.cn/sites/main/preview/bdgg_preview.htm?tid=14012

本周要闻速递

1. 谷歌修复 9 个 Chrome 17 漏洞

北京时间 3 月 23 日消息，据国外媒体报道，谷歌针对 Chrome 17 发布了第六轮安全更新，修复了其中包含的 9 个漏洞。在谷歌修复的这 9 个漏洞中，有 6 个漏洞的安全评级为“高”，有 1 个漏洞的安全评级为“中等”，有 2 个漏洞的安全评级为“低”。目前，Windows、Mac OS X 和 Linux 用户均可以在谷歌网站下载该公司针对 Chrome 17 发布的更新，当前运行 Chrome 浏览器的用户将能够通过后台更新服务获得新版本的自动更新。

参考链接：<http://www.newhua.com/2012/0323/151838.shtml>

2. iPhone 被曝存在漏洞 可使私密照片曝光

据纽约时报报道，苹果最新的漏洞可能会泄露用户的私人相册，用户的秘密照片也将不再安全。与之前读取用户通讯录而没有任何通知一样，用户 iPhone、iPad 以及 iPod 上的私人相册也会被读取，同时没有任何提示信息。根据开发人员透露，一旦你允许苹果的 APP 获取你的地址信息，那么这样的 APP 将在没有任何警告的情况下将复制你私密相册的所有照片。目前还不清楚是否有 APP 非法复制用户的照片。尽管苹果没有特殊的条文禁止这种行为，但是在进入 APP 商店的流程中，苹果会盯着类似于这种明显的不法行为。目前苹果没有对相关问题做出回应。当 APP 第一次要获得你的地理信息时，会有一个提示信息“请求你的允许使用你相册与视频里信息。当用户保存某个相册文件或者视频文件时，与此相关的一些地理坐标信息就会被自动拿走。一位 APP 开发者说：“可以想象得到，获得你允许获取相关地址信息的 APP 将会同时获取你所有摄像地址的历史，这些历史数据与相册和视频都将被上传到服务器。一旦这些信息脱离苹果的设备，苹果就没有能力进行监控或者限制。”

参考链接：http://www.cnhan.com/content/2012-03/22/content_1389559.htm

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