

信息安全漏洞周报

2012 年 3 月 26 日-2012 年 4 月 1 日

2012 年第 13 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 111 个，其中高危漏洞 46 个、中危漏洞 63 个、低危漏洞 2 个。上述漏洞中，可利用来实施远程攻击的漏洞有 108 个。本周收录的漏洞中，已有 69 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“D-Link DCS-5605 PTZ ActiveX 控件'SelectDirectory()'方法缓冲区溢出漏洞”、“Ricoh Company DC Software DL-10 'USER'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 111 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，国内漏洞研究者（个人报送者）向 CNVD 报送了 5 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	79	0
绿盟科技	62	0
天融信	27	0
安天实验室天	25	0
恒安嘉新	24	0
东软	3	0
安氏领信	4	0
个人上报者	5	5

报送总计	229	5
总计	111（去重）	5

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Cisco、Google、Opera、Wireshark、HP 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	Cisco	13	11.7%
2	Google	8	7.2%
3	Opera Software	5	4.5%
4	Wireshark	4	3.6%
5	SWTOR CharDB	3	2.7%
6	HP	3	2.7%
7	Barracuda Networks	2	1.8%
8	Quest Software	2	1.8%
9	Adobe	2	1.8%
10	Joomla!	2	1.8%
11	其它	67	60.4%

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 111 个漏洞。其中操作系统漏洞 16 个，应用程序漏洞 67 个，WEB 应用漏洞 25 个，网络设备漏洞 16 个，数据库漏洞 0 个，安全产品漏洞 0 个。

漏洞影响对象类型	漏洞数量
操作系统漏洞	16
应用程序漏洞	67
WEB 应用漏洞	25
网络设备漏洞	16
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

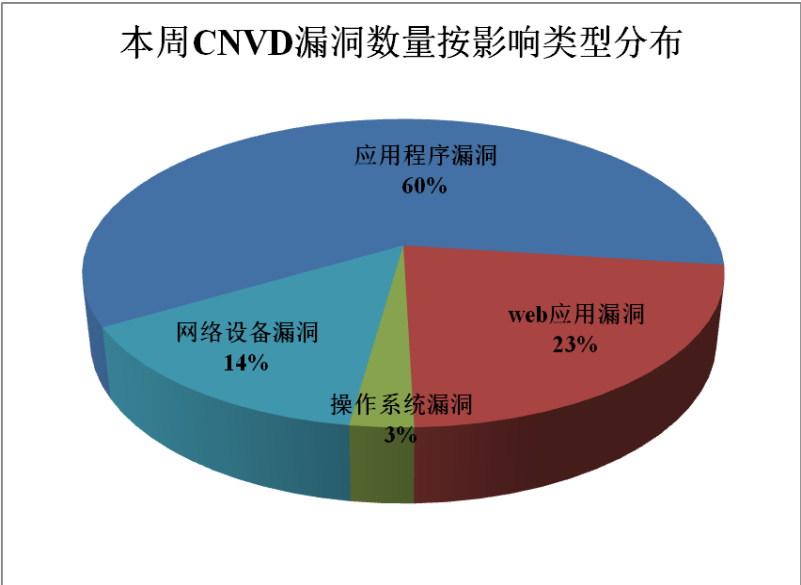


图 1 本周漏洞按影响类型分布



本周涉及电信行业漏洞信息

本周，CNVD 收录了 16 个网络设备漏洞，其中，“D-Link DCS-5605 PTZ ActiveX 控件'SelectDirectory()'方法缓冲区溢出漏洞”和 13 个 Cisco IOS 设备漏洞的综合评级为“高危”。 “D-Link DIR-605 宽带路由器跨站请求伪造漏洞”和 “Sitecom WLM-2501 跨站请求伪造漏洞”的综合评级为“中危”。目前，互联网上已经出现针对“D-Link DCS-5605 PTZ ActiveX 控件'SelectDirectory()'方法缓冲区溢出漏洞”和 “Sitecom WLM-2501 跨站请求伪造漏洞”的攻击代码。

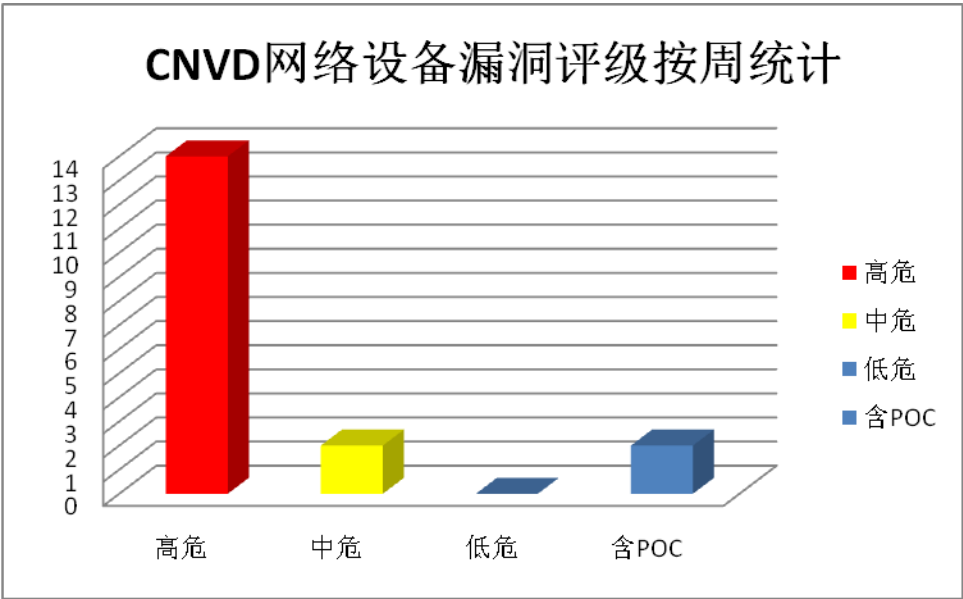


图 2 网络设备漏洞统计



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、Cisco IOS 安全漏洞

Cisco IOS（全称为 Internetwork Operating System）是一款用于思科公司网络设备产品的操作系统。本周，Cisco IOS 被披露存在多个安全漏洞，攻击者可以对任意监听的 UDP 端口进行攻击，或通过会话绕过授权执行任意命令，或利用漏洞进行拒绝服务攻击。CNVD 收录的相关漏洞包括：Cisco Internet 密钥交换（IKE）远程拒绝服务漏洞、Cisco IOS 授权安全绕过漏洞、Cisco IOS RSVP 功能远程拒绝服务漏洞、Cisco IOS MACE 拒绝服务漏洞（CNVD-2012-10941）、Cisco IOS 基于区域的防火墙远程拒绝服务漏洞（CNVD-2012-10951）、Cisco IOS 组播源发现协议远程拒绝服务漏洞、Cisco IOS Smart Install 远程拒绝服务漏洞、Cisco IOS NAT 功能 SIP 远程拒绝服务漏洞。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=46335
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=46338
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=46375
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=46235
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=46277
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=46355
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=46356
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=46357

2、Opera Web Browser 安全漏洞

Opera 是一款开源的 WEB 浏览器。本周，Opera Web Browser 被披露存在多个安全漏洞，攻击者可以利用漏洞绕过跨域策略限制，窃取敏感信息。CNVD 收录的相关漏洞包括：Opera Web Browser 存在多个漏洞（CNVD-2012-10909、CNVD-2012-10910、CNVD-2012-10911、CNVD-2012-10914、CNVD-2012-10913）。其中，“Opera Web Browser 漏洞（CNVD-2012-10909）”和“Opera Web Browser 漏洞（CNVD-2012-10910）”的综合评级为“高危”。目前，Opera Software 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=46036
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=46035
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=46055
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=46037
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=46039

3、Wireshark 安全漏洞

Wireshark 是一款开源的网络协议分析工具。本周，Wireshark 被披露存在多个安全漏洞，攻击者可以利用漏洞发起拒绝服务攻击。CNVD 收录的相关漏洞包括：Wireshark 'call_dissector()'空指针引用拒绝服务漏洞、Wireshark 'ERF'数据拒绝服务漏洞、Wireshark IEEE 802.11 解析器无限循环拒绝服务漏洞、Wireshark MP2T 解析器拒绝服务漏洞。除“Wireshark IEEE 802.11 解析器无限循环拒绝服务漏洞”之外，其余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=46076
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=46097
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=46095
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=46096

4、HP 产品安全漏洞

HP Performance Manager 是一款监视服务器、客户端性能的应用软件；HP-UX（全称为 Hewlett Packard UniX）是一款用于惠普公司服务器产品的操作系统。本周，上述 HP 产品被披露存在多个漏洞，未授权的攻击者可以利用漏洞窃取敏感数据或执行任意代码。CNVD 收录的相关漏洞包括：HP Performance Manager 存在未明远程代码执行漏洞、HP-UX WBEM 本地未授权访问漏洞、HP-UX WBEM 远程未授权访问漏洞。其中，“HP Performance Manager 存在未明远程代码执行漏洞”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=46296
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=46298
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=46058

5、D-Link DCS-5605 PTZ ActiveX 控件>SelectDirectory()方法缓冲区溢出漏洞

D-Link DCS-5605 是一款用于远程监控的网络设备。本周，该产品被披露存在一个缓冲区溢出漏洞。由于用户在浏览设备 WEB 接口时，会被要求安装 Active 控件以查看视频流内容，但控件包含 DcsCliCtrl.dll使用了不安全的 SelectDirectory()函数和 lstrcpW()函数，导致提交畸型参数时会触发栈缓冲区溢出。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=46337

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-2012-10945	Joomla!可预测密码生成漏洞	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通过密码重置功能可猜测生成的密码信息： http://www.joomla.org/
CNVD-2012-10938	TRENDnet TV-IP121WN ActiveX 控件'OpenFileDialog()'方法缓冲区溢出漏洞	高	暂无
CNVD-2012-10950	Novell iManager 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。避免当恶意数据被查看时可以浏览器上下文执行，或导致 SQL 注入攻击： http://www.novell.com/products/consoles/imaganager/overview.html
CNVD-2012-10959	eGroupware 存在多个输入验证漏洞	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。避免泄露敏感信息，或未授权控制应用程序： http://www.egroupware.org/
CNVD-2012-10912	FreePBX Recordings 接口远程代码执行漏洞	高	暂无
CNVD-2012-10918	NextBBS 存在多个 SQL 注入漏洞	高	暂无
CNVD-2012-10864	Apache Traffic Server HTTP Host 头处理堆缓冲区溢出漏洞	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使应用程序崩溃或以应用程序上下文执行任意代码： http://trafficserver.apache.org/download
CNVD-2012-10867	MMPlayer '.m3u'和'.ppl'文件缓冲区溢出漏洞	高	暂无
CNVD-2012-10870	phpFox 'ajax.php'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漏洞以 WEB 权限执行任意 PHP 代码： http://www.phpfox.com/
CNVD-2012-10973	IrfanView Bitmap 文件远程堆缓冲区溢出漏洞	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权限执行任意代码： http://www.irfanview.com/plugins.htm

表 3 部分高危漏洞列表

小结：本周，Cisco 产品被披露存在多个安全漏洞，攻击者可以利用漏洞执行任意代码和拒绝服务等攻击。HP 的多款产品也被披露存在漏洞，未授权的攻击者可以利用漏洞窃取敏感数据或执行任意代码。Opera 浏览器和 Wireshark 软件也被披露存在多个

漏洞。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。D-Link DCS-5605 存在的零日漏洞在互联网上出现了攻击代码，也需引起相关用户的注意。

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、Adobe 发布升级程序，修补 Flash Player 安全漏洞

本周，Adobe 发布升级程序，修补了 Flash Player 存在的安全漏洞。Windows、Macintosh、Linux、Solaris 以及 Android 平台下的 Adobe Flash Player 相关 URL 安全域存在内存破坏漏洞。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=14871

http://www.cnvd.org.cn/sites/main/preview/bdgg_preview.htm?tid=14872

本周要闻速递

1. Android 系统被披露存在服务漏洞 可被黑客利用

日前，国外研究人员发现了 Android 系统存在一个严重漏洞，该漏洞可以被黑客利用发起 DoS 攻击，导致移动设备完全瘫痪。之后，发现该漏洞的研究团队已为 Android 系统打上了补丁。据了解，该漏洞利用程序针对 Android 系统 Linux 层面的 Zygote 套接字(socket)，迫使系统进行资源分配从而发起大量虚拟进程访问请求，从而最终消耗掉设备的全部内存资源。研究小组表示，当 DoS 攻击发生时，用户会发现系统的反应速度不断下降，最终崩溃并重启。虽然设备崩溃之后会试着重新启动，但是研究人员表示，真正的攻击者会设计一种能够调用 DoSChecker 程序的恶意软件，并在启动时被系统自动加载，从而导致设备不断崩溃和重启。这一问题的解决办法是用户手动检查并卸载这一软件，或者给设备重新刷机。除了测试较早的系统，研究人员还在模拟设备上测试了安卓 4.0 和 4.0.3 版本，结果同样如此。相关研究人员已把漏洞及其解决办法发给了 Android 系统安全小组。此外，由于这一漏洞可能造成的潜在巨大安全事件，谷歌将会在最近一次的 Android 系统更新中加入对应的补丁。

参考链接：<http://it.enorth.com.cn/system/2012/03/28/008936525.shtml>

2.微软 Office 漏洞被利用 影响 Mac 系统

据国外媒体报道，日前安全研究人员发现一种利用了微软 Office 漏洞基于电子邮件的攻击，在 Mac 系统上安装远程控制特洛伊木马程序。这种邮件依靠微软 Word 文档，

利用了专为 Mac 系统设计的微软 Office 程序的远程代码执行漏洞，这种攻击将会广泛传播。对于那些没有及时更新微软 Office 版本的用户，这种攻击将会非常有效。一旦攻击得手，黑客可以远程操纵恶意软件来下载，上传和删除文件，或者在系统中打开远程 Shell。安全人员建议 Mac 用户及时更新所使用的软件，特别是一些常用的应用程序，同时保持反病毒软件的持续运行。

参考链接: http://news.ccidnet.com/art/11099/20120330/3732071_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