国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2013 年 03 月 18 日-2013 年 03 月 24 日 **2013 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 118 个，其中高危漏洞 50 个、中危漏洞 59 个、低危漏洞 9 个。上述漏洞中，可利用来实施远程攻击的漏洞有 94 个。本周收录的漏洞中，已有 84 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“Sami FTP Server PUT 命令处理远程溢出漏洞”、“Cisco Video Surveillance Operations Manager 存在多个漏洞”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及个人报送了本周收录的全部 119 个漏洞。各单位报送情况如表 1 所示。其中，恒安嘉新、绿盟科技、启明星辰和天融信等单位报送数量较多。此外，奇虎公司以及个人报送者向 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
启明星辰	35	0
绿盟科技	97	0
安天实验室	18	0
天融信	22	0
恒安嘉新	42	0
奇虎 360	1	1
杭州安恒信息技术有限公司	1	1
个人	2	2
报送总计	218	4

录入总计	119（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 Apple、Linux、HP、Microsoft 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	15	13%
2	Linux	14	12%
3	HP	14	12%
4	Microsoft	6	5%
5	Google	5	4%
6	WordPress	5	4%
7	Ruby on Rails	5	4%
8	RubyGems	4	3%
9	SAP	4	3%
10	Cisco	3	3%
11	其它	43	37%

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 119 个漏洞。其中应用程序漏洞 79 个，WEB 应用漏洞 12 个，操作系统漏洞 23 个，网络设备漏洞 3 个，数据库漏洞 1 个，安全产品 1 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	79
WEB 应用漏洞	12
网络设备漏洞	3
操作系统漏洞	22
数据库漏洞	1
安全产品漏洞	1

表 3 漏洞按影响类型统计表

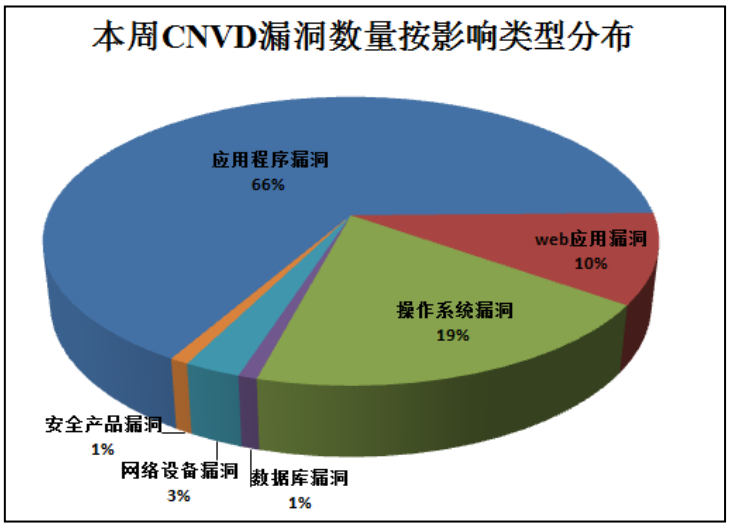

图 1 本周漏洞按影响类型分布

本周涉及电信行业漏洞信息

本周，CNVD 收录了 3 个网络设备漏洞：NEC 多个 aterm 路由器跨站请求伪造漏洞、Cisco IOS 和 IOS XE 不安全密码哈希漏洞、TP-LINK TL-WR740N 路由器拒绝服务漏洞。其中“TP-LINK TL-WR740N 路由器拒绝服务漏洞”互联网上已经出现了针对相关厂商产品的攻击代码，且厂商未发布漏洞的修补程序。

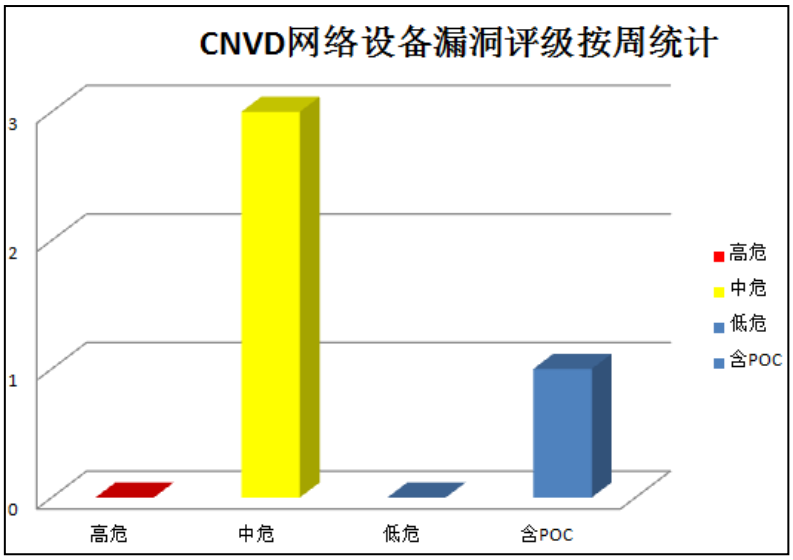

图 2 网络设备漏洞统计

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 产品安全漏洞

Apple iOS 是苹果公司推出的操作系统。本周，上述产品被披露存在多个安全漏洞，攻击者利用漏洞可绕过安全限制，获得敏感信息或远程执行任意代码。

CNVD 收录的相关漏洞包括：Apple iPhone/iPad/iPod touch iOS 信息泄露漏洞、Apple iPhone/iPad/iPod touch iOS 本地任意代码执行漏洞、Apple iPhone/iPad/iPod touch iOS 本地安全绕过漏洞（CNVD-2013-20938、CNVD-2013-20940）、Apple iPhone/iPad/iPod touch iOS 锁屏安全绕过漏洞。厂商已发布了上述漏洞的修补程序。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/flaw/show/CNVD-2013-20932
http://www.cnvd.org.cn/flaw/show/CNVD-2013-20937
http://www.cnvd.org.cn/flaw/show/CNVD-2013-20938
http://www.cnvd.org.cn/flaw/show/CNVD-2013-20940
http://www.cnvd.org.cn/flaw/show/CNVD-2013-20942

2、Linux Kernel 安全漏洞

Linux Kernel 是 Linux 操作系统的内核。本周，该产品被披露存在多个安全漏洞，攻击者利用漏洞泄露敏感信息，执行任意代码或破坏内核内存。

CNVD 收录的相关漏洞包括：Linux Kernel 'cdc-wdm' USB 设备驱动程序堆缓冲区溢出漏洞、Linux Kernel Netlink Interface 存在多个信息泄露漏洞、Linux Kernel ext3 信息记录格式串漏洞 、Linux Kernel KVM 'MSR_KVM_SYSTEM_TIME'内存错误引用内存破坏漏洞、Linux Kernel KVM 拒绝服务漏洞、Linux Kernel KVM 缓冲区溢出漏洞。上述漏洞中“Linux Kernel KVM 'MSR_KVM_SYSTEM_TIME'内存错误引用内存破坏漏洞”、“Linux Kernel KVM 缓冲区溢出漏洞”的综合评级均为“高危”。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/flaw/show/CNVD-2013-20903
http://www.cnvd.org.cn/flaw/show/CNVD-2013-21057
http://www.cnvd.org.cn/flaw/show/CNVD-2013-21059
http://www.cnvd.org.cn/flaw/show/CNVD-2013-21060
http://www.cnvd.org.cn/flaw/show/CNVD-2013-21061
http://www.cnvd.org.cn/flaw/show/CNVD-2013-21062

3、IBM 产品安全漏洞

本周，IBM 多款产品 Tivoli Endpoint Manager、Rational ClearQuest、Sterling Order Management、InfoSphere Information Server 被披露存在多个安全漏洞，攻击者利用漏洞获得敏感信息。

CNVD 收录的相关漏洞包括：IBM InfoSphere Information Server 不安全文件权限漏洞、IBM Sterling Order Management XPath 注入漏洞、IBM Sterling Order Management 存

在未明跨站脚本漏洞、IBM Rational ClearQuest 跨站脚本漏洞（CNVD-2013-21031）、IBM Tivoli Endpoint Manager 跨站脚本漏洞（CNVD-2013-21039 ）。上述漏洞中“IBM InfoSphere Information Server 不安全文件权限漏洞”的综合评级均为“高危”。厂商已发布上述漏洞的修补程序。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/flaw/show/CNVD-2013-20917
http://www.cnvd.org.cn/flaw/show/CNVD-2013-20945
http://www.cnvd.org.cn/flaw/show/CNVD-2013-20946
http://www.cnvd.org.cn/flaw/show/CNVD-2013-21031
http://www.cnvd.org.cn/flaw/show/CNVD-2013-21039

4、HP 产品安全漏洞

HP Intelligent Management Center 是一款惠普公司发行的智能管理应用程序。本周，该产品被披露存在多个安全漏洞，攻击者利用漏洞获得敏感信息或执行任意脚本代码。

CNVD 收录的相关漏洞包括： HP 产品远程执行代码漏洞、HP 产品远程信息泄露漏洞（CNVD-2013-20885、CNVD-2013-20886、CNVD-2013-20892、CNVD-2013-20893、CNVD-2013-20894、CNVD-2013-20895、CNVD-2013-20896）。上述漏洞的综合评级均为“高危”。厂商已发布了上述漏洞的修补程序。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/flaw/show/CNVD-2013-20884
http://www.cnvd.org.cn/flaw/show/CNVD-2013-20885
http://www.cnvd.org.cn/flaw/show/CNVD-2013-20886
http://www.cnvd.org.cn/flaw/show/CNVD-2013-20892
http://www.cnvd.org.cn/flaw/show/CNVD-2013-20893
http://www.cnvd.org.cn/flaw/show/CNVD-2013-20894
http://www.cnvd.org.cn/flaw/show/CNVD-2013-20895
http://www.cnvd.org.cn/flaw/show/CNVD-2013-20896

5、Sami FTP Server PUT 命令处理远程溢出漏洞

Sami FTP Server 是一款 FTP 服务程序。本周，该产品被披露存在一个综合评级为“高危”的溢出漏洞。攻击者利用漏洞使应用程序崩溃或执行任意代码。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/flaw/show/CNVD-2013-20979

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/flaw/list.htm

CNVD 编号	漏洞名称	综合评级	修复方式
CNVD-2013-21016	VxWorks SSH server (IPSSH)拒绝服务漏洞（CNVD-2013-21016）	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://jvn.jp/en/jp/JVN20671901/index.html
CNVD-2013-20988	Aktiv Player '.wma'文件拒绝服务漏洞	高	暂无
CNVD-2013-20986	OpenCart 'filemanager.php'存在多个目录遍历漏洞	高	暂无
CNVD-2013-20983	yaSSL 存在未明缓冲区溢出漏洞（CNVD-2013-20983）	高	用户可联系供应商获得补丁信息：http://www.yassl.com/
CNVD-2013-20978	Google Picasa BMP 文件处理堆缓冲区溢出漏洞	高	用户可参考如下厂商获得最新的升级程序：http://picasa.google.com/
CNVD-2013-20977	EA Origin 任意代码执行漏洞	高	目前厂商还没有提供此漏洞的相关补丁或者升级程序，建议使用此软件的用户随时关注厂商的主页以获取最新版本：https://www.origin.com/ie/download
CNVD-2013-20976	DjVuLibre '.djv'文件内存破坏漏洞	高	DjVuLibre 3.5.25.3 已经修复此漏洞，建议用户下载更新：http://djvu.sourceforge.net/
CNVD-2013-20960	RubyGems 'command_wrap'远程命令执行漏洞	高	暂无
CNVD-2013-20947	Photodex ProShow Producer 本地权限提升漏洞	高	暂无
CNVD-2013-20931	ossec 口令配置文件权限绕过漏洞	高	暂无

表 3 部分高危漏洞列表

小结：本周，Apple iOS 和 Linux Kernel 被披露存在多个漏洞，攻击者利用漏洞可获得敏感信息或远程执行任意代码、破坏内核内存。HP 和 IBM 的多款产品也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或执行任意脚本代码，对企业用户构成较大威胁。此外，国内应用较多的 Sami FTP Server 被披露存在零日漏洞，相关用户应随时关注厂商主页，及时获取修复补丁或解决方案。

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、Real Networks 发布升级程序，修补 RealPlayer 安全漏洞

RealNetworks RealPlayer 是一款流行的媒体播放程序。本周，RealNetworks 发布升级程序，修补了 RealPlayer 存在的漏洞。远程攻击者可利用漏洞以应用程序上下文执行任意代码。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/patchInfo/show/32941

本周要闻速递

1. 苹果被爆重大安全漏洞

综合英国《每日邮报》和美国《洛杉矶时报》报道，美国专利与商标局(USPTO)周四公开了苹果提交的一项专利申请，该项专利旨在防止 iPhone 等电子设备跌落后被摔坏。然而与此同时，苹果公司系统再度传出重大安全漏洞，据说通过漏洞可轻易修改别人苹果账号的密码并绑架账户。据美国《洛杉矶时报》报道，一个科技新闻网站宣称发现这个网路教学影片。影片告诉使用者如何通过修改后的苹果网址进入别人的苹果账户并重置密码。基于安全考量，该网站未公布教学影片链接，但建议使用者启动苹果账户的两步骤安全验证机制，以保护账号。

参考链接：http://www.northnews.cn/2013/0325/1072022.shtml

2. 三星 Galaxy Note2 存在安全漏洞

最近三星的几款设备相机被曝光存在安全隐患，而最近开发者 Terence Eden 再次发现了 Galaxy Note II 的锁屏漏洞，能够绕过现有的锁屏机制，在跳转到紧急拨号界面时候会闪过解锁后的画面。随后他发现目前这个漏洞只适用于运行 Android 4.1.2 的国际版 Note2 和运行 4.1.1 的 AT&T 版 Note II，至于 Galaxy S3 其他 Android 设备则不受影响。Eden 的这种方式需要耐心，但是在几次尝试之后就能非常轻松的找到相关的诀窍，成功的概率也将会大大提升。当消费者返回到解锁界面的时候，消费者能够看到为解锁的画面一闪而过，而你要抓住这个机会按 Home 按键就能直接进入到桌面。

参考链接：http://tech.cnr.cn/list/201303/t20130321_512198891.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