

信息安全漏洞周报

2013 年 04 月 29 日-2013 年 05 月 05 日

2013 年第 18 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低。

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 82 个，其中高危漏洞 39 个、中危漏洞 36 个、低危漏洞 7 个。上述漏洞中，可利用来实施远程攻击的漏洞有 72 个。本周收录的漏洞中，已有 62 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“SMF 'index.php' PHP 注入漏洞”、“Light HTTPD 栈缓冲区溢出漏洞（CNVD-2013-23483）”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 82 个漏洞。各单位报送情况如表 1 所示。其中，启明星辰、安天实验室、天融信等单位报送数量较多。此外，奇虎公司、High-Tech Bridge Security Research Lab 以及个人报送者向 CNVD 提交了 19 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	90	0
绿盟科技	35	0
安天实验室	61	0
天融信	60	0
恒安嘉新	11	0
奇虎 360	2	2
High-Tech Bridge Security Research Lab	1	1
个人	16	16

报送总计	276	19
录入总计	82（去重）	19

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、Joomla!、phpMyAdmin、Linux 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	10	12%
2	Joomla!	8	10%
3	phpMyAdmin	4	5%
4	Linux	4	5%
5	WordPress	3	4%
6	HP	3	4%
7	IBM	2	2%
8	McAfee	2	2%
9	Apache	2	2%
10	Citrix	2	2%
11	其它	42	52%

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 82 个漏洞。其中应用程序漏洞 36 个，WEB 应用漏洞 31 个，操作系统漏洞 4 个，网络设备漏洞 9 个，安全产品漏洞 2 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	36
WEB 应用漏洞	31
网络设备漏洞	9
操作系统漏洞	4
安全产品漏洞	2
数据库漏洞	0

表 3 漏洞按影响类型统计表

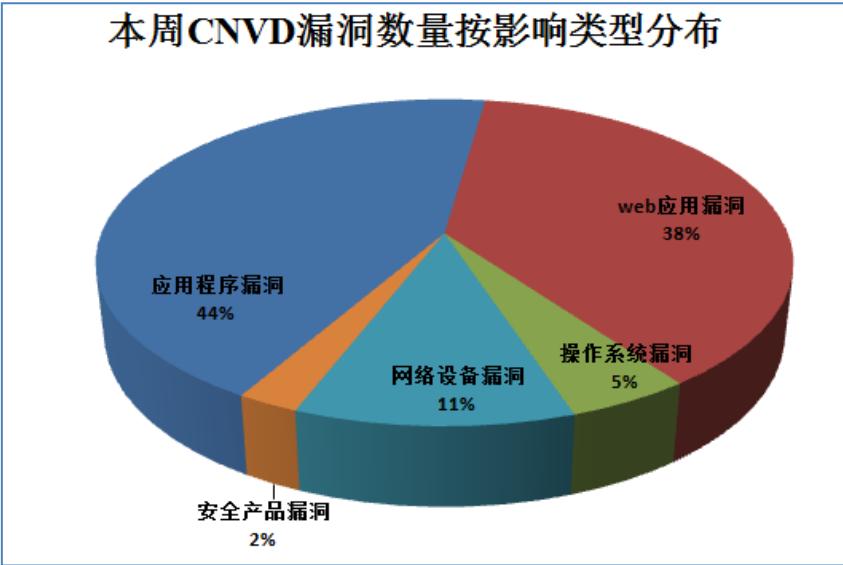


图 1 本周漏洞按影响类型分布

本周涉及电信行业漏洞信息

本周,CNVD 收录了 9 个网络设备漏洞: HP ElitePad 900 PCs with BIOS 配置漏洞、多个 Cisco 产品 Jumbo 报文拒绝服务漏洞、多个 Cisco 产品 CDP 子系统缓冲区溢出漏洞、多个 Cisco 产品 SNMP 和许可证管理程序缓冲区溢出漏洞、多个 Cisco 产品 SNMP 缓冲区溢出漏洞、Citrix NetScaler 和 Access Gateway 未授权访问漏洞、D-Link DIR-635 存在多个漏洞、多个 HP LaserJet Printers 信息泄露漏洞、HP Managed Printing Administration 跨站脚本漏洞。除“Citrix NetScaler 和 Access Gateway 未授权访问漏洞、D-Link DIR-635 存在多个漏洞”之外,其余漏洞的综合评级均为“高危”。相关厂商已经发布了漏洞修补程序。

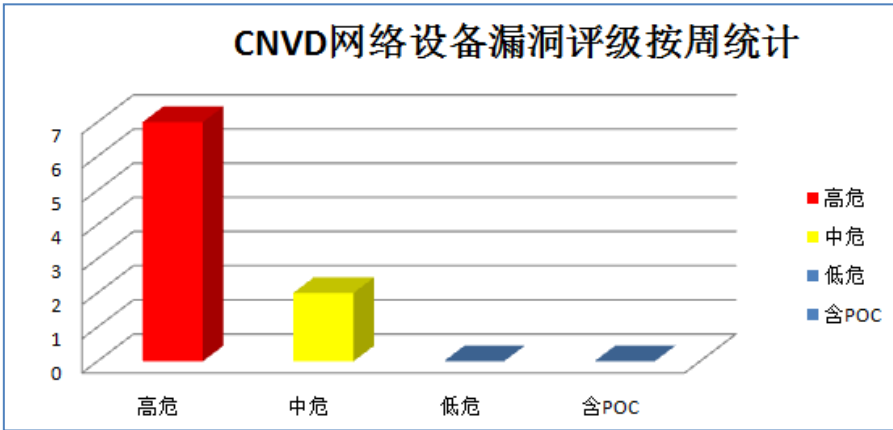


图 2 网络设备漏洞统计

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、Cisco 产品安全漏洞

Cisco Unified Communications 是一款 Cisco IP 电话解决方案中的呼叫处理组件；Cisco Nexus 7000 是一种模块化的数据中心级交换机；Cisco Intrusion Prevention System (IPS) 是网络攻击检测设备。本周，上述产品被披露存在多个安全漏洞，攻击者利用漏洞可获得敏感信息，劫持用户会话，发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Cisco Unified Communications Domain Manager 存在未明跨站脚本漏洞、Cisco Nexus 7000 系列交换机拒绝服务漏洞、Cisco IOS XR SNMP 模块内存泄露拒绝服务漏洞、Cisco Intrusion Prevention System 本地拒绝服务漏洞。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-2013-23620>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-23619>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-23618>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-23617>

2、D-LINK 产品安全漏洞

本周，多个 D-Link 网络摄像头产品被披露存在安全漏洞，攻击者利用漏洞可获得敏感信息和未授权的访问，执行任意命令。

CNVD 收录的相关漏洞包括：多个 D-LINK 产品内置账户安全绕过漏洞、多个 D-LINK 产品命令注入漏洞、多个 D-LINK 产品信息泄露漏洞（CNVD-2013-23650、CNVD-2013-23649）、多个 D-LINK 产品验证绕过漏洞。其中，“多个 D-LINK 产品内置账户安全绕过漏洞、多个 D-LINK 产品命令注入漏洞”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-2013-23652>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-23646>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-23650>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-23649>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-23648>

3、IBM 产品安全漏洞

IBM SPSS SamplePower 是一款统计分析软件；IBM Sametime links 是一款企业级实时协作的平台。本周，上述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，执行任意代码。

CNVD 收录的相关漏洞包括：IBM SPSS SamplePower 'vsflex7l' ActiveX 控件任意代码执行漏洞、IBM SPSS SamplePower 'c1sizer' ActiveX 控件缓冲区溢出漏洞、IBM SPSS

SamplePower 'vsflex8l' ActiveX 控件任意代码执行漏洞、IBM SPSS SamplePower ActiveX 控件任意代码执行漏洞、IBM Sametime 客户端实现命令发送漏洞、IBM Sametime 跨站脚本漏洞、IBM Connections 跨站脚本漏洞。其中，“IBM SPSS SamplePower 'vsflex7l' ActiveX 控件任意代码执行漏洞、IBM SPSS SamplePower 'c1sizer' ActiveX 控件缓冲区溢出漏洞、IBM SPSS SamplePower 'vsflex8l' ActiveX 控件任意代码执行漏洞、IBM SPSS SamplePower ActiveX 控件任意代码执行漏洞”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-2013-23632>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-23630>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-23629>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-23605>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-23604>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-23603>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-23601>

4、BOINC 产品安全漏洞

BOINC 全称为伯克利开放式网络计算平台，是开放的用于志愿计算和网格计算的中间件系统。本周，该产品被披露存在多个安全漏洞，攻击者利用漏洞可更改数据库信息或控制应用系统，使应用程序崩溃，执行任意命令。

CNVD 收录的相关漏洞包括：BOINC SQL 注入漏洞、BOINC XML 解析器栈缓冲区溢出漏洞、BOINC 元素解析栈缓冲区溢出漏洞。其中，“BOINC SQL 注入漏洞”的综合评级为“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-2013-23614>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-23615>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-23613>

5、Light HTTPD 栈缓冲区溢出漏洞（CNVD-2013-23483）

Light HTTPD 是一款开源 Web 服务器软件。本周，该产品被披露存在一个综合评级为“高危”的缓冲区溢出漏洞。由于 Windows 下的 Light HTTPD 未能正确处理用户提交的输入，远程攻击者利用漏洞提交恶意请求触发基于栈的缓冲区溢出，可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-2013-23483>

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-2013-23571	VMWare vCenter Server 验证安全绕过漏洞	高	vCenter Server 5.1 update1 已经修复此漏洞, 建议用户下载更新: https://downloads.vmware.com/d/info/datacenter_cloud_infrastructure/vmware_vsphere/5_1
CNVD-2013-23598	Henry Schein Dentrux G5 内置密码安全绕过漏洞	高	Dentrux G5 version 15.1.294 已经修复此漏洞, 建议用户下载使用: http://www.dentrux.com/support/software-updates/g5.aspx
CNVD-2013-23621	Elecard MPEG Player '.m3u'文件缓冲区溢出漏洞	高	暂无
CNVD-2013-23624	FoeCMS 'item.php' SQL 注入漏洞	高	暂无
CNVD-2013-23628	Galil RIO-47100 'Pocket PLC'组件拒绝服务漏洞	高	用户可联系厂商获得相应的升级或补丁程序: http://www.galilmc.com/support/firmware-downloads.php
CNVD-2013-23645	WPS Office 'Wpsio.dll'栈缓冲区溢出漏洞	高	暂无
CNVD-2013-23638	多个 MatrikonOPC 产品目录遍历漏洞	高	用户可联系厂商获得相应的升级或补丁程序: http://www.matrikonopc.com/login/index.aspx
CNVD-2013-23641	FreePBX 'page.backup.php'脚本远程命令执行漏洞	高	FreePBX 2.10 已经修复此漏洞, 建议用户下载更新: http://www.freepbx.org
CNVD-2013-23640	WebKit 内存错误引用远程代码执行漏洞	高	用户可参考如下厂商提供的安全公告获得补丁信息: http://trac.webkit.org/changeset/149185

表 3 部分高危漏洞列表

小结: 本周, Cisco 多款产品被披露存在多个拒绝服务漏洞, 主要影响涉及基础电信企业和相关企业用户, BOINC 以及 IBM 多款产品被披露存在多个漏洞, 攻击者利用漏洞可执行任意代码, 渗透信息系统。D-LINK 多款网络摄像头产品被披露存在多个权限绕过漏洞, 个人用户需注意防范。此外, Light HTTPD 被披露存在零日漏洞, 相关网站管理员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、Apache 发布升级程序，修补 CloudStack 产品安全漏洞

Apache CloudStack 是部署和管理大型虚拟机网络的开源软件。本周，Apache 发布升级程序，修补了 CloudStack 存在的漏洞。攻击者可获得敏感信息并获得未经授权访问任意用户的控制台。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/33644>

<http://www.cnvd.org.cn/patchInfo/show/33643>

本周要闻速递

1. 微软证实 IE8 存在 0day 漏洞

微软上周五证实 IE8 中存在一个 0day 漏洞，可导致远程代码执行。据多家安全机构证实，该漏洞已经被用来攻击用户，例如，美国劳工部和美国能源部遭受的 Watering hole 式攻击。微软日前发布了一个安全公告，承认该漏洞的存在，不过此漏洞仅影响 IE8，并不会影响 IE6、IE7、IE9、IE10。微软表示正在开发安全更新来修复这个漏洞，但是并未提供明确的时间表。建议 Vista 和 Win7 用户升级至 IE9 或 IE10，如果你不愿意升级至更新版本的 IE，可将 Internet 和本地区域安全设置为“高”；或者将 IE8 设置为运行任何 Active Script 类型的程序前均提醒用户，或者直接禁用 Active Scripting。

参考链接：<http://news.mydrivers.com/1/262/262416.htm>

2. 三星手机被指有重大漏洞

据国外媒体报道，一位开发者近日在论坛曝出，三星 Exynos 4 系列处理器上存有重大漏洞，黑客可利用此漏洞使手机瘫痪。媒体引用此开发者帖子表示，出现此安全漏洞的设备均搭载有三星 Exynos 4210 或 4412 处理器。黑客可利用此漏洞进入手机的物理内存，更改或盗取用户数据。对此三星 Galaxy S 和 Note 系列手机以及魅族 MX/MX2 等搭载 Exynos 4 系列处理器的终端都有可能受影响。据了解，开发者现已经将该漏洞报告给三星，但是对此漏洞的修补方法，三星暂时还未披露，不过经检查 Exynos 5 系列处理器上则没有发现这个漏洞。

参考链接：http://fashion.eastday.com/consumer_life/20130506/82090.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