

信息安全漏洞周报

2013 年 04 月 22 日-2013 年 04 月 28 日

2013 年第 17 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 138 个，其中高危漏洞 29 个、中危漏洞 81 个、低危漏洞 28 个。上述漏洞中，可利用来实施远程攻击的漏洞有 111 个。本周收录的漏洞中，已有 83 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“NETGEAR DGND3700 'ping.cgi'远程命令执行漏洞”、“ZPanel 'templateparser.class.php' PHP 代码注入漏洞”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 7 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 138 个漏洞。各单位报送情况如表 1 所示。其中，启明星辰、安天实验室等单位报送数量较多。此外，湖北分中心、奇虎公司以及个人报送者向 CNVD 提交了 23 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	130	0
绿盟科技	74	0
安天实验室	120	0
天融信	62	0
恒安嘉新	35	0
奇虎 360	7	7
东软	2	0
CNCERT 湖北分中心	2	2
个人	14	14

报送总计	446	23
录入总计	138（去重）	23

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Linux、Belkin、D-LINK、Netgear 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	Linux	17	12%
2	Belkin	10	7%
3	D-LINK	9	7%
4	Netgear	7	5%
5	Cisco	6	4%
6	IBM	5	4%
7	TP-LINK	4	3%
8	WordPress	4	3%
9	Apache	3	2%
10	Fork CMS	3	2%
11	其它	70	51%

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 138 个漏洞。其中应用程序漏洞 58 个，WEB 应用漏洞 28 个，操作系统漏洞 17 个，网络设备漏洞 32 个，安全产品漏洞 3 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	58
WEB 应用漏洞	28
网络设备漏洞	32
操作系统漏洞	17
安全产品漏洞	3
数据库漏洞	0

表 3 漏洞按影响类型统计表

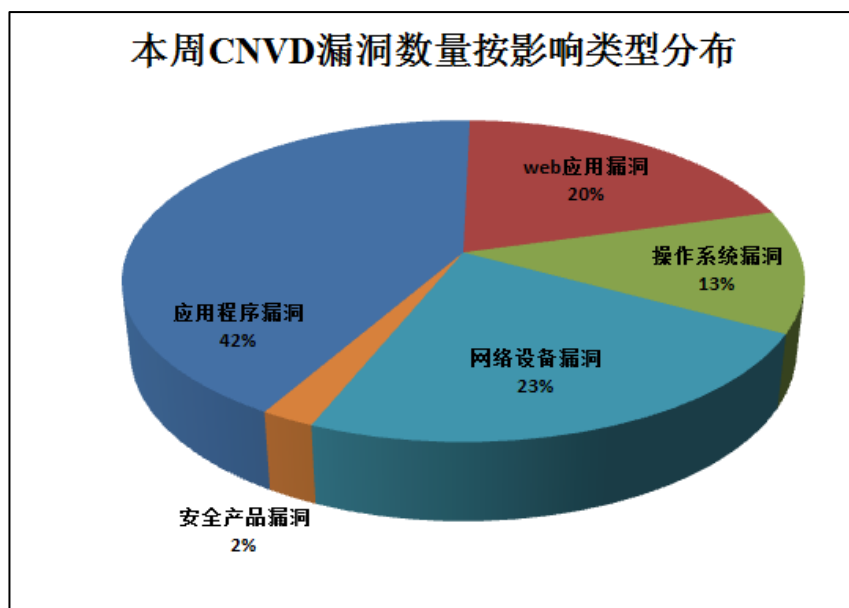


图 1 本周漏洞按影响类型分布

本周涉及电信行业漏洞信息

本周，CNVD 收录了 32 个网络设备漏洞：Belkin 产品漏洞 6 个，D-Link 设备漏洞 9 个，Linksys 产品漏洞 2 个，Netgear 产品漏洞 8 个，TP-LINK 产品漏洞 4 个，Ruckus 产品漏洞 1 个、Verizon 产品漏洞 1 个，Cisco IOS 漏洞 1 个。其中，“Cisco IOS 通用输入/输出 SNMP 查询远程拒绝服务漏洞、D-LINK DIR-615/DIR-300 OS 命令注入漏洞、D-LINK DIR-615/DIR-300 密码更改漏洞、NETGEAR DGND3700 'ping.cgi'远程命令执行漏洞”的综合评级均为“高危”。目前，互联网上已经出现了针对“D-Link DIR-865L 跨站请求伪造漏洞、TP-LINK TL-WR741N/TL-WR741ND 路由器拒绝服务漏洞、D-LINK DIR-615/DIR-300 OS 命令注入漏洞、D-LINK DIR-615/DIR-300 HTTP 标头注入漏洞、D-LINK DIR-615/DIR-300 敏感信息泄露漏洞、NETGEAR DGND3700 'ping.cgi'远程命令执行漏洞”的攻击代码，相关厂商已经发布了漏洞修补程序。

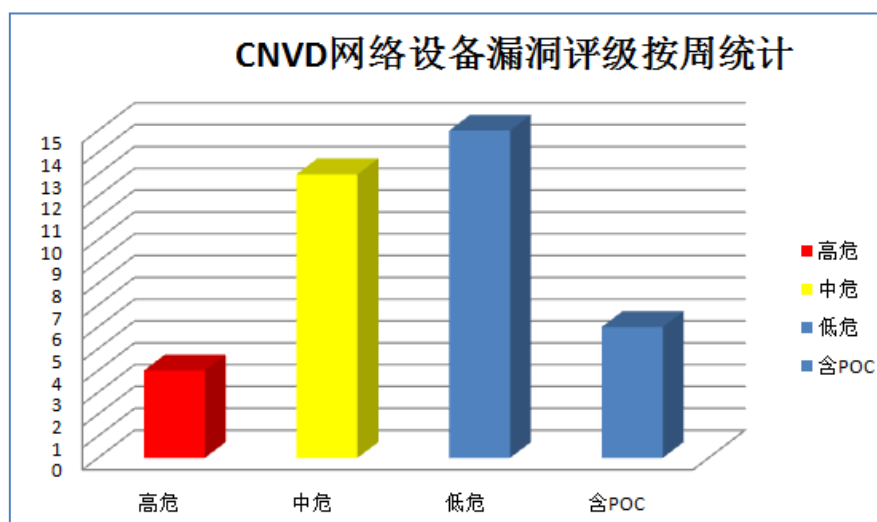


图 2 网络设备漏洞统计

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 Device Manager 是思科路由器基于 Web 的设备管理工具；Cisco IOS 是一款为其网络设备开发的操作系统；Cisco Adaptive Security Appliance 提供安全和 VPN 服务的模块；Cisco Unified Contact Center Express 是一款联系中心解决方案。本周，上述产品被披露存在多个安全漏洞，攻击者利用漏洞可提升权限，导致设备重载。

CNVD 收录的相关漏洞包括：Cisco Device Manager 存在多个远程命令执行漏洞、Cisco IOS 通用输入/输出 SNMP 查询远程拒绝服务漏洞、Cisco Adaptive Security Appliance Time-Range 对象安全绕过漏洞、Cisco Unified Contact Center Express 信息泄露漏洞、Cisco ASA 无客户 SSL VPN CIFS 远程拒绝服务漏洞、Cisco ASA Software VPN 组枚举漏洞。其中，“Cisco Device Manager 存在多个远程命令执行漏洞、Cisco IOS 通用输入/输出 SNMP 查询远程拒绝服务漏洞”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-2013-23217>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-23120>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-23113>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-23106>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-22683>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-22682>

2、D-LINK 产品安全漏洞

D-LINK DIR-615/DIR-300 是一款无线路由器设备；D-Link DIR-865L 是一款企业级无线路由设备。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，执行任意操作。

CNVD 收录的相关漏洞包括：D-LINK DIR-615/DIR-300 密码更改漏洞、D-LINK DIR-615/DIR-300 OS 命令注入漏洞、D-LINK DIR-615/DIR-300 敏感信息泄露漏洞、D-LINK DIR-615/DIR-300 HTTP 标头注入漏洞、D-LINK DIR-615/DIR-300 反射型跨站脚本漏洞、D-LINK DIR-615/DIR-300 不安全加密存储漏洞、D-LINK DIR-615/DIR-300 跨站请求伪造漏洞、D-Link DIR-865L 存在未明硬件链接漏洞等。其中，“D-LINK DIR-615/DIR-300 密码更改漏洞、D-LINK DIR-615/DIR-300 OS 命令注入漏洞”的综合评级均为“高危”。除“D-Link DIR-865L 存在未明硬件链接漏洞”外，厂商已发布其余漏洞的修补程序。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-2013-23220>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-23219>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-23226>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-23225>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-23223>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-23222>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-23221>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-23047>

3、Linux 产品安全漏洞

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，攻击者利用漏洞获得敏感信息。

CNVD 收录的相关漏洞包括：Linux kernel 'VSOCK'子系统 vmci 内存信息泄露漏洞、Linux kernel 'VSOCK'子系统内存信息泄露漏洞、Linux kernel 'tipc'子系统内存信息泄露漏洞、Linux kernel 'Bluetooth'子系统 SCO 内存信息泄露漏洞、Linux kernel 'rose'子系统内存信息泄露漏洞、Linux kernel 'Bluetooth'子系统 RFCOMM 内存信息泄露漏洞、Linux kernel 'netrom'子系统内存信息泄露漏洞、Linux kernel 'llc'子系统内存信息泄露漏洞等。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-2013-23157>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-23154>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-23153>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-23152>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-23151>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-23150>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-23149>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-23146>

4、Netgear 产品安全漏洞

Netgear DGND3700/WNDR4700 是一款无线路由器设备。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，执行任意命令，发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：NETGEAR DGND3700 'ping.cgi'远程命令执行漏洞、Netgear WNDR4700 媒体服务器存在未明拒绝服务漏洞、Netgear WNDR4700 存在未明 SMB 符号链接目录遍历漏洞、Netgear WNDR4700 存在未明未授权硬件链接漏洞、Netgear WNDR4700 验证绕过漏洞、Netgear WNDR4700 存在未明信息泄露漏洞（CNVD-2013-23058、CNVD-2013-23056）、Netgear WNDR4700 跨站脚本漏洞。其中，“NETGEAR DGND3700 'ping.cgi'远程命令执行漏洞”的综合评级为“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-2013-23234>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-23062>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-23061>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-23060>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-23059>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-23058>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-23057>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-23056>

5、ZPanel 'templateparser.class.php' PHP 代码注入漏洞

ZPanel 是一款免费的虚拟主机控制面板。本周，该产品被披露存在一个综合评级为“高危”的代码注入漏洞。由于 ZPanel 'templateparser.class.php'未能正确过滤用户提交的恶意代码，远程攻击者利用漏洞可注入恶意代码，并结合 ZPanels `zsudo`程序，以 root 权限执行任意命令。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-2013-22702>

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-2013-23231	Hornbill Supportworks ITSM 组件 SQL 注入漏洞	高	ITSM 最新版本已修复此漏洞，建议用户下载使用：

			http://www.hornbill.com/
CNVD-2013-23230	tinc 'receive_tcp packet()'缓冲区溢出漏洞	高	tinc 1.0.21 已经修复此漏洞，建议用户下载更新： http://www.tinc-vpn.org/
CNVD-2013-23224	GroundWork monarch_scan.cgi OS 命令执行漏洞	高	暂无
CNVD-2013-23229	WebKit 'CompositeEditCommand::cloneParagraphUnderNewElement'内存错误引用漏洞	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/148908 https://src.chromium.org/viewvc/blink?revision=148680&view=revision
CNVD-2013-23216	Joomla Civicrm 组件任意 shell 上传漏洞	高	暂无
CNVD-2013-23215	ERDAS ER Viewer 'ERM_convert_to_correct_webpath()'缓冲区溢出漏洞	高	ERDAS ER Viewer 13.00.0001 及之后版本已经修复此漏洞，建议用户下载更新： http://geospatial.intergraph.com/products/other/erdasermapper/ERDASERViewer/Details.aspx
CNVD-2013-23211	Oracle Java 小程序反射类型混淆远程代码执行漏洞	高	暂无
CNVD-2013-23134	Global Mapper 不安全库加载代码执行漏洞	高	暂无
CNVD-2013-23133	vBilling 存在多个 SQL 注入漏洞	高	暂无
CNVD-2013-23122	FirePHP Add-on for Firefox 数组数据 cell 名处理任意代码执行漏洞	高	FirePHP Add-on for Firefox 0.7.2 已经修复此漏洞，建议用户下载使用： http://firephp.org/

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漏洞，主要影响基础电信运营商和相关企业用户，而 D-LINK、Netgear 等无线路由器产品存在的多个漏洞则有可能影响企业及个人用户信息和网络运行安全。Linux Kernel 被披露存在多个漏洞，攻击者利用漏洞获得敏感信息。此外，ZPanel 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。

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 ActiveMQ 产品安全漏洞

Apache ActiveMQ 是一款开源消息总线，用于支持 JMS1.1 和 J2EE 1.4 规范的 JMS Provider 实现。本周，Apache 发布升级程序，修补了 ActiveMQ 存在的漏洞。远程攻击者可利用漏洞获得敏感信息或进行拒绝服务攻击。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/33599>

<http://www.cnvd.org.cn/patchInfo/show/33598>

<http://www.cnvd.org.cn/patchInfo/show/33597>

本周要闻速递

1. Java 漏洞出现大量攻击

安全公司 F-Secure 发布通告，有恶意软件正在利用甲骨文（Oracle）上周才刚修补的漏洞展开大量攻击，因此使用者应立即更新 Java 至最新版本 Java 7 Update 21。另一方面，也有安全专家在 Java 7 Update 21 中又找到新的漏洞。研究人员发现一个叫 Reveton 的勒索软件利用此次更新的漏洞进行攻击，该软件会锁住电脑操作系统，然后以使用非法软件或非法下载为借口，要求缴交罚金。

参考链接：<http://www.donews.com/it/201304/1484874.shtml>

2. 寻找 Chrome 浏览器漏洞可获 3 万美元奖励

近日传出消息，谷歌公司给一位研究员支付了 31336 美元。据称，这位来自卢森堡大学的研究员维曼，由于帮助谷歌解决了 Chrome 浏览器的程序漏洞而受到奖赏。在今年春季，谷歌已经总共在 Chrome 和 Chrome OS 问题排除悬赏中支付了将近 18.8 万美元的奖励金。但是，这次针对维曼的奖励格外丰厚一些。谷歌官方表示，他们很高兴维曼能帮助他们解决谷歌 Chromium 浏览器的易损问题，这位研究院还帮谷歌排除了三大连串的漏洞，其中包括演示开发代码和非常复杂的编写。这种贡献值得这 3 万多美元的奖励。

参考链接：<http://it.21cn.com/itnews/a/2013/0501/05/21400344.shtml>

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