

信息安全漏洞周报

2015 年 03 月 02 日-2015 年 03 月 08 日

2015 年第 10 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 133 个，其中高危漏洞 25 个、中危漏洞 100 个、低危漏洞 8 个。上述漏洞中，可利用来实施远程攻击的漏洞有 124 个。本周收录的漏洞中，已有 91 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。其中互联网上出现“D-Link DCS-931L with firmware 无限制文件上传漏洞”、“HelpDEZk 存在多个漏洞”等零日攻击代码，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 5 家成员单位及个人报送了本周收录的全部 133 个漏洞。报送情况如表 1 所示。其中，奇虎 360、安天实验室、启明星辰、天融信、恒安嘉新等单位报送数量较多。此外，补天平台、CNCERT 各分中心、北京安信天行科技有限公司及白帽子向 CNVD 提交了 774 个原创漏洞。

报送单位或个人	漏洞报送数量	原创漏洞数量
奇虎 360	754	754
安天实验室	195	0
启明星辰	74	0
天融信	64	0
恒安嘉新	53	0
北京安信天行科技有限公司	1	1

CNCERT 福建分中心	2	2
CNCERT 宁夏分中心	2	2
CNCERT 甘肃分中心	1	1
个人	14	14
报送总计	1160	774
录入总计	133（去重）	774

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Drupal、WordPress、Cisco 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	Drupal	16	12%
2	WordPress	11	8%
3	Cisco	8	6%
4	D-Link	6	5%
5	Loxone	6	5%
6	IBM	5	4%
7	PNMsoft	4	3%
8	tisa	3	2%
9	GNU	3	2%
10	其他	71	53%

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 133 个漏洞。其中应用程序漏洞 74 个，WEB 应用漏洞 45 个，网络设备漏洞 9 个，操作系统漏洞 3 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	74
WEB 应用漏洞	45
网络设备漏洞	9
操作系统漏洞	3

安全产品漏洞	2
--------	---

表 3 漏洞按影响类型统计表

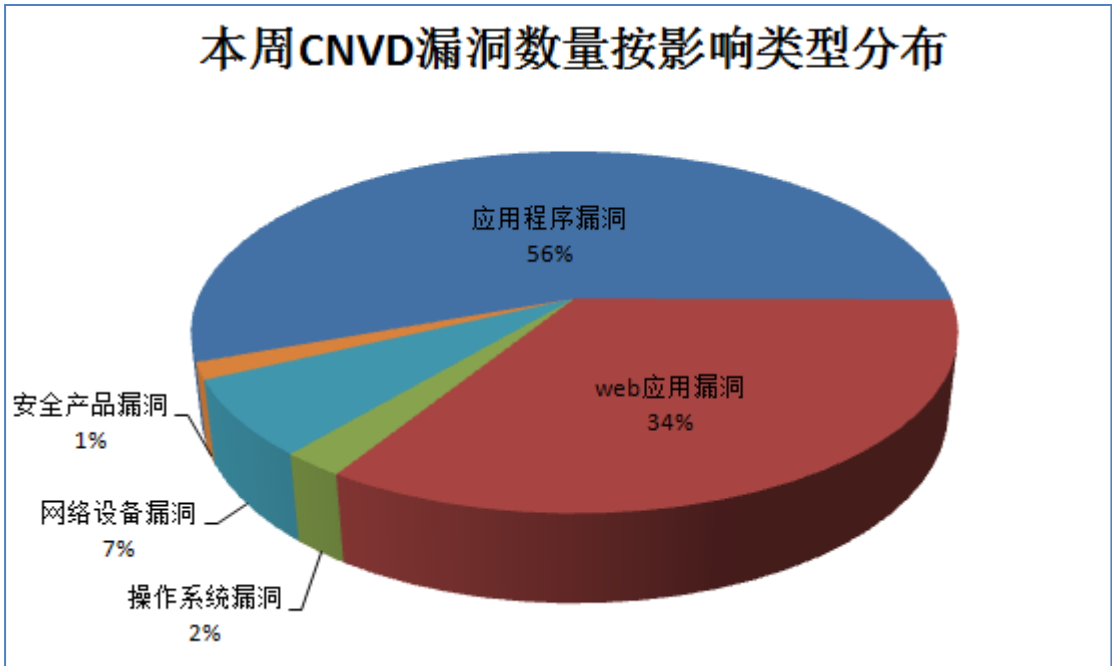


图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 8 个电信行业漏洞，2 个移动互联网行业漏洞（如下图表所示）。其中，“D-Link DIR-645 Wired/Wireless Router 栈缓冲区溢出漏洞、D-Link DIR-645 Wired/Wireless Router 操作系统命令注入漏洞、多个 D-Link 和 TRENDnet 路由器'ncc/nc c2' Service 存在多个漏洞”的综合评级均为“高危”。相关厂商已经发布了上述漏洞的修补程序。

行业	漏洞编号	漏洞标题	危险等级	是否有补丁
电信	CNVD-2015-01376	D-Link DIR-645 Wired/Wireless Router 栈缓冲区溢出漏洞	高	是
电信	CNVD-2015-01373	D-Link DIR-645 Wired/Wireless Router 操作系统命令注入漏洞	高	是
电信	CNVD-2015-01395	SEIL 路由器 PPP Access Concentrator 拒绝服务漏洞	中	是
电信	CNVD-2015-01406	Cisco Security Manager 存在多个跨站脚本漏洞	中	是
电信	CNVD-2015-01407	Cisco IOS Software 安全绕过漏洞	中	是
电信	CNVD-2015-01409	Cisco Application Networking Manager 跨站请求伪造漏洞	中	是
电信	CNVD-2015-01410	Cisco IOS/IOS XE Software 拒绝服务	中	是

		漏洞		
电信	CNVD-2015-01453	多个 D-Link 和 TRENDnet 路由器'ncc/nc c2' Service 存在多个漏洞	高	是
移动互联网	CNVD-2015-01361	Speed Software Root Explorer 目录遍历漏洞	中	是
移动互联网	CNVD-2015-01424	Google Play services 信息泄露漏洞	中	是

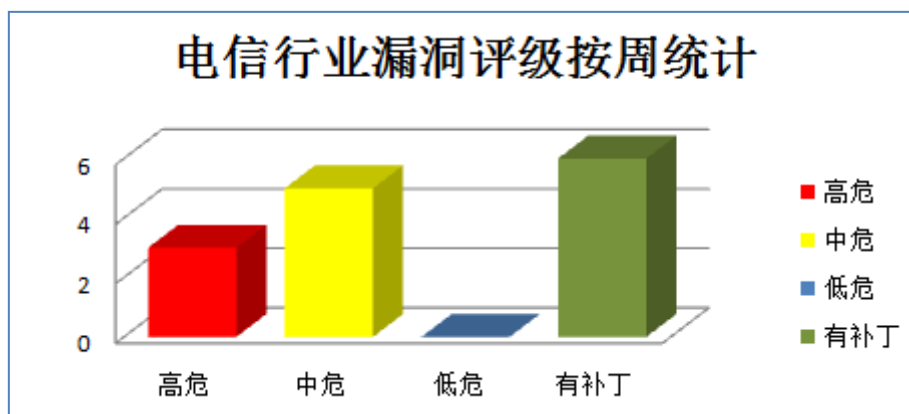


图 1 电信行业漏洞统计

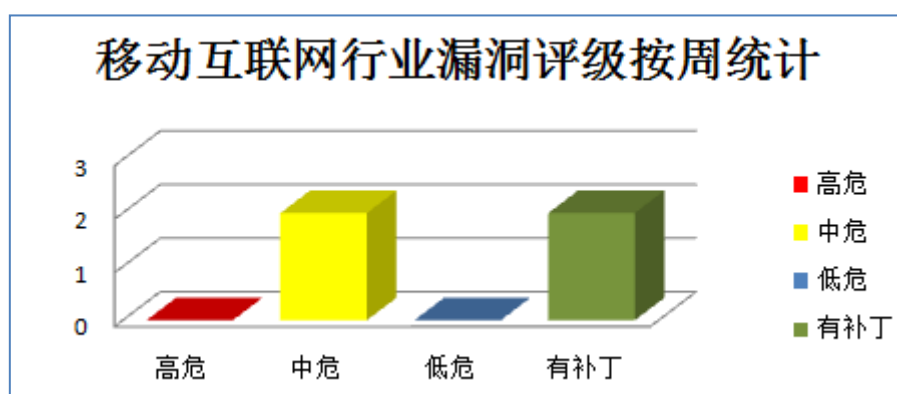


图 2 移动互联网行业漏洞统计

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 Web 和 E-mail Interaction Manager 都是美国思科（Cisco）公司的客户协作联系中心中的产品。Cisco IOS 是多数思科系统路由器和网络交换机上使用的互连网络操作系统。Cisco Application Networking Manager 是美国思科（Cisco）公司一套网络应用管理工具。Cisco Security Manager 可将配置策略的任务和针对思科安全部署的控制措施集中起来处理，从而能够高效地管理企业级安全性。Cisco Unified Comp

uting System 通过将统一计算、网络、存储访问和虚拟化整合到一个系统中，简化 IT 管理并提高灵活性。本周，上述产品被披露存在跨站脚本、安全绕过和拒绝服务漏洞，攻击者可利用漏洞进行跨站脚本攻击、执行未经授权操作或发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Cisco IOS XR Software IPv6 报文处理拒绝服务漏洞、Cisco Network Analysis Module 跨站脚本漏洞、Cisco Unified Web Interaction Manager 跨站脚本漏洞、Cisco IOS/IOS XE Software 拒绝服务漏洞、Cisco Application Networking Manager 跨站请求伪造漏洞、Cisco IOS Software 安全绕过漏洞、Cisco Security Manager 存在多个跨站脚本漏洞、Cisco Unified Computing System C-Series DHCP 报文处理拒绝服务漏洞。其中，“Cisco IOS XR Software IPv6 报文处理拒绝服务漏洞”的综合评级为“高危”。除“Cisco Network Analysis Module 跨站脚本漏洞”外，厂商已经发布了其余漏洞的修补程序。CNVD 提醒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-2015-01353>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-01451>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-01392>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-01410>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-01409>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-01407>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-01406>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-01364>

2、Drupal 产品安全漏洞

Drupal 是 Drupal 社区所维护的一套用 PHP 语言开发的免费、开源的内容管理系统。本周，上述产品被披露存在跨站脚本和跨站请求伪造漏洞，攻击者可利用漏洞进行跨站脚本攻击或执行未经授权操作。

CNVD 收录的相关漏洞包括：Drupal Node Access Product 模块跨站脚本漏洞、Drupal Feature Set 模块跨站请求伪造漏洞、Drupal Ubercart Webform Integration 模存在多个跨站脚本漏洞、Drupal Custom Sitemap 模块跨站请求伪造漏洞、Drupal Watchdog Aggregator 模块跨站请求伪造漏洞、Drupal SMS Framework Module 跨站脚本漏洞、Drupal Entity API 模块字段标签跨站脚本漏洞、Drupal inLinks Integration 模块跨站脚本漏洞。目前，厂商已经发布了“Drupal SMS Framework Module 跨站脚本漏洞、Drupal Entity API 模块字段标签跨站脚本漏洞”漏洞的修补程序。CNVD 提醒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-2015-01464>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-01465>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-01415>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-01438>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-01457>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-01416>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-01456>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-01413>

3、D-Link 产品安全漏洞

D-Link DCS-931L 是 D-Link 家用无线网络摄像机。D-Link DIR-645 是友讯（D-Link）公司的一款可调节无线发射功率的路由器产品。D-Link DAP-1320 是友讯（D-Link）公司的一款无线网络延伸器产品。本周，上述产品被披露存在多个安全漏洞，攻击者可利用漏洞进行未授权操作或执行任意代码。

CNVD 收录的相关漏洞包括：D-Link DCS-931L with firmware 无限制文件上传漏洞、D-Link DIR-645 Wired/Wireless Router 操作系统命令注入漏洞、D-Link DAP-1320 代码注入漏洞、D-Link DCS-931L 跨站请求伪造漏洞、D-Link DIR-645 Wired/Wireless Router 栈缓冲区溢出漏洞。其中，除“D-Link DCS-931L 跨站请求伪造漏洞”外，其余漏洞的综合评级为“高危”。目前，厂商已经发布了除“D-Link DCS-931L with firmware 无限制文件上传漏洞”外，其余漏洞的修补程序。CNVD 提醒用户及时下载补丁更新，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-2015-01423>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-01373>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-01374>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-01375>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-01376>

4、IBM 产品安全漏洞

IBM Maximo Asset Management 是美国 IBM 公司的一套 IT 资产管理解决方案。IBM Rational Insight 是美国 IBM 公司的一款企业级报表应用产品，它可以将第三方产品中的数据抽取到数据仓库，利用运行在 WebSphere 上的 CognosBI 服务，将报表用图形方式展现出来。本周，上述产品被披露存在多个安全漏洞，攻击者可利用漏洞获取敏感信息、进行跨站脚本攻击或执行未授权操作。

CNVD 收录的相关漏洞包括：IBM Maximo Asset Management 跨站脚本漏洞、IBM Maximo Asset Management 跨站脚本漏洞（CNVD-2015-01431）、IBM Maximo Asset Management 目录遍历漏洞、IBM Maximo Asset Management 访问限制绕过漏洞、IBM Rational Insight 信息泄露漏洞。目前，厂商已经发布了上述漏洞的修补程序。CNVD 提醒用户及时下载补丁更新，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-2015-01430>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-01431>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-01425>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-01426>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-01382>

5、HelpDEZk 存在多个漏洞

HelpDEZk 是一套基于 PHP 的用于管理请求、事件的软件。该软件通过一个共享服务中心管理工作流程、记录流程及维护历史记录等。本周，HelpDEZk 被披露存在综合评级为“高危”的任意文件上传、命令执行和信息泄露漏洞。攻击者可以利用漏洞获取敏感信息，执行任意命令，或上传任意文件到受影响应用程序。目前，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-2015-01441>

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-2015-01349	PHP 内存错误引用远程代码执行漏洞	高	PHP 5.4.38, 5.5.22 或 5.6.6 已经修复该漏洞，建议用户下载更新： http://php.net
CNVD-2015-01377	Zhone GPON 2520 输入验证漏洞	高	目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接： http://www.zhone.com/support/manuals/docs/830/830-02004-02.pdf
CNVD-2015-01397	KENT-WEB Joyful Note 任意代码执行漏洞	高	目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接： http://www.kent-web.com/bbs/joyful.html
CNVD-2015-01399	GNU glibc 'getaddrinfo.c' 远程代码执行漏洞	高	目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载： http://www.gnu.org/software/libc/
CNVD-2015-01400	GNU glibc 'fnmatch_loop.c' 远程缓冲区溢出漏洞	高	用户可以联系供应商获得补丁信息： http://www.gnu.org/software/libc/
CNVD-2015-01401	GNU C Library 拒绝服务漏洞	高	用户可参考如下厂商提供的安全公告获取补丁以修复该漏洞： http://lists.opensuse.org/opensuse-updates/2015-02/msg00089.html
CNVD-2015-01420	JBPM jbpm-designer XML 外部实体漏洞	高	目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接： https://rhn.redhat.com/errata/RHSA-2015-0234.html

CNVD-2015-01421	Infoblox Network Automation NetMRI Anyterm Daemon 任意命令执行漏洞	高	目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接： https://support.infoblox.com/app/answers/detail/a_id/3666/kw/NETMRI-23483
CNVD-2015-01422	ClipBucket SQL 注入漏洞	高	用户可参考如下厂商提供的安全公告获取补丁以修复该漏洞： http://osvdb.org/show/osvdb/118667
CNVD-2015-01437	SoftSphere DefenseWall Personal Firewall 权限提升漏洞	高	用户可参考如下厂商提供的安全公告获取补丁以修复该漏洞： http://www.osvdb.org/117996

表 3 部分高危漏洞列表

小结：本周，Cisco 多款产品被披露存在跨站脚本、安全绕过和拒绝服务漏洞，攻击者可利用漏洞进行跨站脚本攻击、执行未经授权操作或发起拒绝服务攻击。此外，Drupal、D-Link、IBM 多款产品被披露存在多个安全漏洞，允许攻击者利用漏洞获取敏感信息、进行跨站攻击、执行未经授权操作或执行任意代码。另外，HelpDEZk 被披露存在一个高危零日漏洞，攻击者可利用漏洞获取敏感信息，执行任意命令，或上传任意文件。建议相关用户应随时关注上述厂商主页，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 修补 Standard Taglibs 产品漏洞

Apache Standard Taglibs 是美国阿帕奇（Apache）软件基金会的一个 JSP 标准标签库（JSTL）规范的实现。

本周，Apache 修补了上述产品存在的 XML 外部实体注入漏洞，避免攻击者利用漏洞在受影响应用程序上下文中执行任意代码。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网络安全事件。

补丁下载链接：<http://www.cnvd.org.cn/patchInfo/show/55870>

本周要闻速递

1. MongoDB phpMoAdmin 曝远程代码执行漏洞

MongoDB 是 IT 行业中流行的一种开源 NoSQL 数据库，其数据存储方式非常灵活，广泛应用于不同规模大小的公司中。其所有的数据持久操作都无需开发人员手动编写 SQL 语句，直接调用方法即可轻松的实现 CRUD 操作。phpMoAdmin 是一个免费、开源、以 PHP 为基础、基于 AJAX 的 MongoDB GUI 管理工具，管理者可轻松管理 NoSQL 数

据库。日前，绰号为 sp1nlock 的黑客在 phpMoAdmin 上发现了一个远程代码执行 0day 漏洞，攻击者可以利用该漏洞劫持运行 phpMoAdmin 工具的网站。

参考链接：<http://www.freebuf.com/news/59972.html>

2. D-Link（友讯）路由器存在远程命令注入漏洞

近日安全研究员在 D-Link（友讯）路由器上发现了一个严重的安全漏洞，首先是 D-Link DIR636L 型号的路由器对“ping”工具上的输入信息过滤不当导致攻击者可以在路由器上注入任意命令；其次是认证机制在执行过程中也出现了错误，所以攻击者可以远程获得设备的 root 权限。基于 ping.ccp 漏洞的属性，用户只要访问嵌入恶意 HTTP form 的网页，攻击者就可获得设备的 root 访问权限，劫持 DNS 设置或者在受害者设备上执行任意命令。

参考链接：<http://www.freebuf.com/news/59861.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

国家计算机网络应急技术处理协调中心（简称“国家互联网应急中心”，英文简称是 CNCERT 或 CNCERT/CC），成立于 2002 年 9 月，为非政府非盈利的网络安全技术中心，是我国网络安全应急体系的核心协调机构。

作为国家级应急中心，CNCERT 的主要职责是：按照“积极预防、及时发现、快速响应、力保恢复”的方针，开展互联网网络安全事件的预防、发现、预警和协调处置等工作，维护国家公共互联网安全，保障基础信息网络和重要信息系统的安全运行。

网址：www.cert.org.cn

邮箱：vreport@cert.org.cn

电话：010-82990999