国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2015 年 11 月 30 日-2015 年 12 月 06 日 **2015 年第 49 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 92 个，其中高危漏洞 62 个、中危漏洞 27 个、低危漏洞 3 个。上述漏洞中，可利用来实施远程攻击的漏洞有 87 个。本周收录的漏洞中，已有 58 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“Oracle Bee Hive 2 voice-servlet prepareAudioToPlay()任意文件上传漏洞”、“Acunetix WVS 本地权限提升漏洞”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 7 家成员单位、合作伙伴及个人报送了本周收录的全部 92 个漏洞。报送情况如表 1 所示。其中，奇虎(补天平台)、安天实验室、启明星辰、恒安嘉新等单位报送数量较多。补天平台、乌云、漏洞盒子及白帽子向 CNVD 提交了 1065 个以事件型漏洞为主的原创漏洞。

报送单位或个人	漏洞报送数量	原创漏洞数量
奇虎(补天平台)	642	642
安天实验室	84	0
启明星辰	56	0
恒安嘉新	46	0
绿盟科技	40	0
天融信	28	0

H3C	3	0
乌云	388	388
漏洞盒子	22	22
High-Tech Bridge Security Research Lab	4	4
CNCERT 海南分中心	2	2
个人	7	7
报送总计	1322	1065
录入总计	92（去重）	1065

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 PCRE、Cisco、D-Link 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	PCRE	16	17%
2	Cisco	6	7%
3	D-Link	5	5%
4	IBM	3	3%
5	RSI Video Technologies	3	3%
6	Cyrus	3	3%
7	QEMU	2	2%
8	Apache	2	2%
9	Epiphany Healthcare	2	2%
10	其他	50	56%

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 92 个漏洞。其中应用程序漏洞 51 个，Web 应用漏洞 27 个，网络设备漏洞 12 个，操作系统漏洞 1 个，安全产品漏洞 1 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	51

Web 应用漏洞	27
网络设备漏洞	12
操作系统漏洞	1
安全产品漏洞	1

表 3 漏洞按影响类型统计表

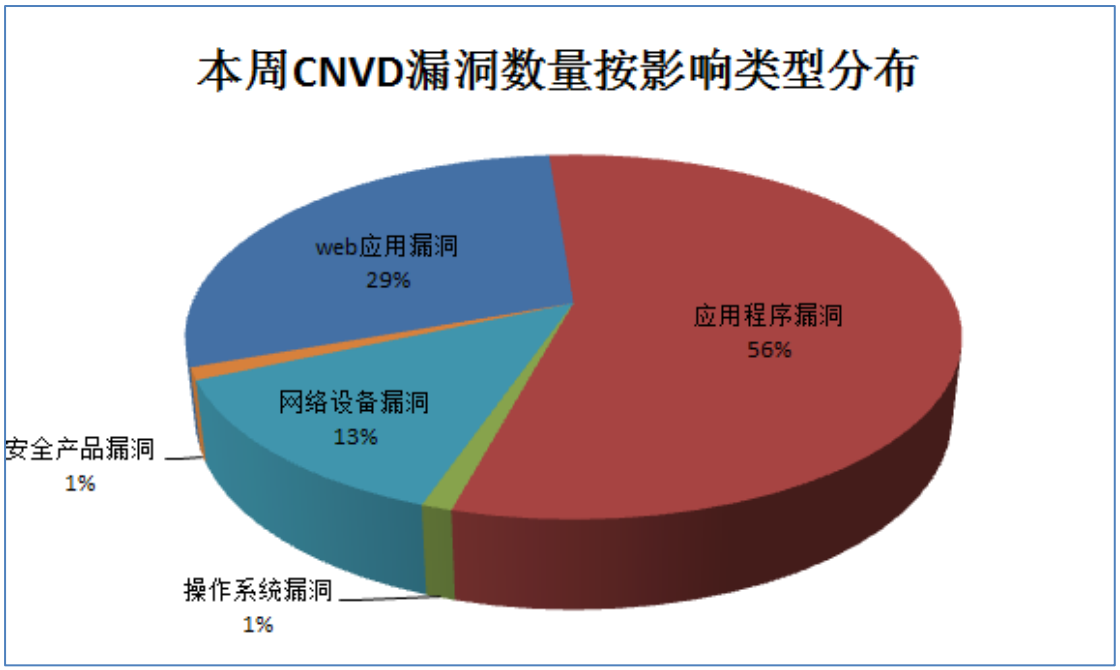

图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 10 个电信行业漏洞、2 个工控系统行业漏洞（如下图表所示）。其中，“多款 IBM 产品密码过期漏洞、Cisco ASR 1000 IOS XE 安全绕过漏洞、Siemens SIMATIC 通信机模块信息泄露漏洞、多款 Saia Burgess Controls 产品 PCD 硬编码密码漏洞”的综合评级为“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-2015-07845	Cisco ASR 5000 Series Telnetd 拒绝服务漏洞	中	否
电信	CNVD-2015-07852	D-Link DIR-890L 和 DIR-890R 缓冲区溢出漏洞	高	否
电信	CNVD-2015-07853	D-Link DIR-866L ‘HNAP’和‘Send Email’功能缓冲区溢出漏洞	高	否
电信	CNVD-2015-07854	D-Link DIR-880L ‘HNAP’和‘Authentication’功能缓冲区溢出漏洞	高	否
电信	CNVD-2015-07855	D-Link DIR-825 存在多个漏洞	高	否
电信	CNVD-2015-07856	D-Link DGL5500 ’HNAP‘功能缓冲区溢出漏洞	高	否

电信	CNVD-2015-07863	多款 Cisco 产品信息泄露漏洞	中	是
电信	CNVD-2015-07873	Cisco Cloud Services Router 1000V 命令注入漏洞	中	是
电信	CNVD-2015-07890	多款 IBM 产品密码过期漏洞	高	是
电信	CNVD-2015-07907	Cisco ASR 1000 IOS XE 安全绕过漏洞	高	是
工控系统	CNVD-2015-07864	Siemens SIMATIC 通信机模块信息泄露漏洞	高	是
工控系统	CNVD-2015-07900	多款 Saia Burgess Controls 产品 PCD 硬编码密码漏洞	高	是

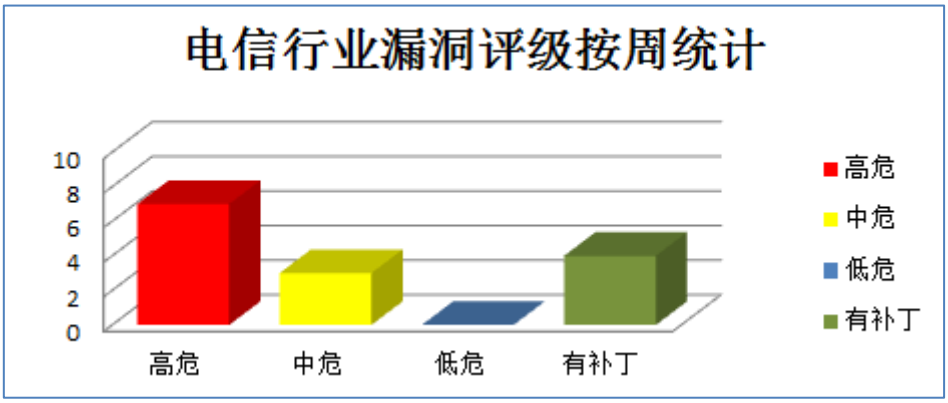

图 1 电信行业漏洞统计

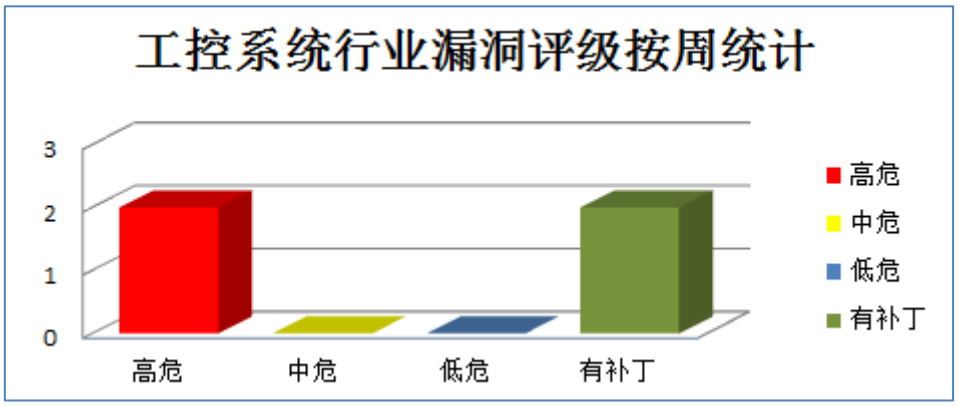

图 2 工控系统行业漏洞统计

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、D-Link 产品安全漏洞

D-Link DIR-825、DGL5500、DIR-890L、DIR-890R、DIR-866L、DIR-880L 是友讯（D-Link）公司的无线路由器产品。本周，上述产品被披露存在目录遍历和缓冲区溢出漏洞。攻击者利用漏洞可获得敏感信息、执行任意代码和发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：D-Link DIR-825 存在多个漏洞、D-Link DGL5500 '

HNAP'功能缓冲区溢出漏洞、D-Link DIR-890L 和 DIR-890R 缓冲区溢出漏洞、D-Link DIR-866L 'HNAP'和'Send Email'功能缓冲区溢出漏洞、D-Link DIR-880L 'HNAP'和'Authentication'功能缓冲区溢出漏洞。上述漏洞的综合评级为“高危”。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-2015-07855

http://www.cnvd.org.cn/flaw/show/CNVD-2015-07856

http://www.cnvd.org.cn/flaw/show/CNVD-2015-07852

http://www.cnvd.org.cn/flaw/show/CNVD-2015-07853

http://www.cnvd.org.cn/flaw/show/CNVD-2015-07854

2、 Cisco 产品安全漏洞

Cisco IOS XE on ASR 1000 是美国思科（Cisco）公司的一套运行于 ASR 1000 系列路由器设备中的操作系统。Cisco Unity Connection 是美国思科（Cisco）公司的一套语音留言平台。该平台可利用语音命令，以“免提”方式拨打电话或者收听留言。Cisco Web Security Appliance 是安全的 Web 网关，在一个平台上集成了恶意软件防护、应用可视化控制、策略控制等。Cisco IOS on Cloud Services Router（CSR）1000V 是美国思科（Cisco）公司一套运行于云服务路由器 1000V 系列产品中的操作系统。Cisco RV320 Dual Gigabit WAN VPN 是美国思科公司的路由器产品。Cisco ASR 5000 系列是一个运营商级平台,可用于部署高需求的 3G 网络以及向长期演进 (LTE) 迁移。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、绕过安全限制、进行跨站脚本攻击、执行命令注入和发起拒绝服务攻击等。

CNVD 收录的相关漏洞包括：Cisco ASR 1000 IOS XE 安全绕过漏洞、Cisco Unity Connection 跨站脚本漏洞、Cisco Web Security Appliance 拒绝服务漏洞（CNVD-2015-07874）、Cisco Cloud Services Router 1000V 命令注入漏洞、多款 Cisco 产品信息泄露漏洞、Cisco ASR 5000 Series Telnetd 拒绝服务漏洞。其中，“Cisco ASR 1000 IOS XE 安全绕过漏洞”的综合评级为“高危”。目前，厂商已经发布了除“Cisco Web Security Appliance 拒绝服务漏洞（CNVD-2015-07874）、Cisco ASR 5000 Series Telnetd 拒绝服务漏洞”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-2015-07907

http://www.cnvd.org.cn/flaw/show/CNVD-2015-07908

http://www.cnvd.org.cn/flaw/show/CNVD-2015-07874

http://www.cnvd.org.cn/flaw/show/CNVD-2015-07873

http://www.cnvd.org.cn/flaw/show/CNVD-2015-07863

http://www.cnvd.org.cn/flaw/show/CNVD-2015-07845

3、 PCRE 产品安全漏洞

PCRE（Perl Compatible Regular Expressions）是软件开发者 Philip Hazel 所研发的一个使用 C 语言编写的开源正则表达式函数库。本周，上述产品被披露存在拒绝服务漏洞。攻击者利用漏洞可发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：PCRE 拒绝服务漏洞（CNVD-2015-07877、CNVD-2015-07876、CNVD-2015-07879、CNVD-2015-07880、CNVD-2015-07881、CNVD-2015-07883、CNVD-2015-07884、CNVD-2015-07885）。上述漏洞的综合评级为“高危”。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-2015-07877
http://www.cnvd.org.cn/flaw/show/CNVD-2015-07876
http://www.cnvd.org.cn/flaw/show/CNVD-2015-07879
http://www.cnvd.org.cn/flaw/show/CNVD-2015-07880
http://www.cnvd.org.cn/flaw/show/CNVD-2015-07881
http://www.cnvd.org.cn/flaw/show/CNVD-2015-07883
http://www.cnvd.org.cn/flaw/show/CNVD-2015-07884
http://www.cnvd.org.cn/flaw/show/CNVD-2015-07885

4、FFmpeg 产品安全漏洞

FFmpeg 是一套可录制、转换以及流化音视频的完整解决方案。本周，上述产品被披露存在整数溢出和拒绝服务漏洞。攻击者利用漏洞可发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：FFmpeg‘jpeg2000_read_main_headers'函数拒绝服务漏洞、FFmpeg 'smka_decode_frame'函数拒绝服务漏洞、FFmpeg 'ff_ivi_init_planes'函数整数溢出漏洞。目前，厂商已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-2015-07850
http://www.cnvd.org.cn/flaw/show/CNVD-2015-07849
http://www.cnvd.org.cn/flaw/show/CNVD-2015-07848

5、Oracle BeeHive 2 voice-servlet prepareAudioToPlay()任意文件上传漏洞

Oracle Beehive 是 Oracle 用于企业消息传递和写作服务的软件平台。本周，Oracle Beehive 被披露存在任意文件上传漏洞。攻击者利用该漏洞可执行任意代码。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-2015-07924

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-2015-07847	EMC IsilonOneFS 操作系统权限提升漏洞	高	用户可联系供应商获得补丁信息：https://sso.emc.com/
CNVD-2015-07851	IBM Cúram Social Program Management SQL 注入漏洞	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.ibm.com/
CNVD-2015-07861	SmokePingsmokeping_cgi 任意代码执行漏洞	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：https://github.com/oetiker/SmokePing
CNVD-2015-07866	CIS Manager 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://www.construtiva.com.br/portal/solucoes/
CNVD-2015-07867	Gwolle Guestbook WordPress 插件远程文件包含漏洞	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：https://wordpress.org/plugins/gwolle-gb/changelog/
CNVD-2015-07875	RSI Video Technologies Frontel 硬编码加密漏洞	高	目前厂商已经发布了升级补丁以修复此安全问题，详情请关注厂商主页：http://www.videofied.com/
CNVD-2015-07878	RSI Video Technologies Frontel 信息泄露漏洞	高	目前厂商已经发布了升级补丁以修复此安全问题，详情请关注厂商主页：http://www.videofied.com/
CNVD-2015-07882	RSI Video Technologies Frontel 数据真实性验证漏洞	高	目前厂商已经发布了升级补丁以修复此安全问题，详情请关注厂商主页：http://www.videofied.com/
CNVD-2015-07890	多款 IBM 产品密码过期漏洞	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-01.ibm.com/support/docview.wss?uid=swg21969052
CNVD-2015-07886	多款 IBM 产品安全绕过漏洞（CNVD-2015-07886）	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-01.ibm.com/support/docview.wss?uid=swg21970799

表 3 部分高危漏洞列表

小结：本周，D-Link 产品被披露存在目录遍历和缓冲区溢出漏洞。攻击者利用漏洞可获得敏感信息、执行任意代码和发起拒绝服务攻击。此外，Cisco、PCRE、FFmpeg 多款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、绕过安全限制、

进行跨站脚本攻击、执行任意代码和发起拒绝服务攻击等。另外，Oracle Beehive 被披露存在一个高危漏洞，攻击者利用该漏洞可执行任意代码。建议相关用户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、HP 修补 Virtual Table Server（VTS）产品漏洞

HP LoadRunner 是一款惠普公司开发的性能测试工具。

本周，HP 修补了上述产品存在的远程代码执行漏洞，避将攻击者利用漏洞执行任意代码。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/67357

本周要闻速递

1. libupnp 漏洞归来影响大量智能系统设备

目前趋势科技（Trend Micro ）发布了一份报告显示，便携式 UPnP 设备 SDK 当中存在一个 3 年之久的安全漏洞，这个被称为 libupnp 的漏洞，出现在数以百万计的智能电视，智能手机和路由器当中。攻击者可以利用这个漏洞在受影响的设备当中触发缓冲区溢出，这反过来会导致远程代码执行。且随着研究的深入发现这个漏洞不仅可以导致设备崩溃，还可以使恶意攻击者在受影响的设备上面远程执行恶意程序，也可使得恶意攻击者有机会远程控制该设备。

参考链接：http://www.freebuf.com/news/88368.html

2. 谷歌被曝秘密收集学生信息

近日，电子前哨基金会（Electronic Frontier Foundation 简称 EFF）向美国联邦贸易委员会(FTC)举报谷歌秘密收集学生的网络数据。谷歌浏览器下的 Chrome 同步功能赋予了谷歌收集学生整个网页浏览历史记录并随意使用的权力。此外，Google 的教育管理员设置功能则不仅让谷歌可以获得学生数据，而且还分享给了第三方网站。这个过程还收集学生们搜索的关键字，他们点击的视频，这些结果全会储存在云服务器上。并且这个过程事先不会征求学生家长的同意，另外有些学校要求学生使用 Chromebook，这样使得学生家长更难阻止这种数据采集的行为。目前，谷歌方面已经向 EFF 表示，他们将很快禁用校园版 Chromebook 中的一个设置功能，这样 Chrome 同步数据就不会再被分享到谷歌其他服务中，如收集浏览网站信息，同步分享功能。虽然这一举措已经得到了 EFF 的认可，但该组织认为谷歌还需要作出更大的变化才行。

参考链接：http://www.freebuf.com/news/87947.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