国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2015 年 12 月 28 日-2016 年 01 月 03 日 **2016 年第 1 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 78 个，其中高危漏洞 24 个、中危漏洞 49 个、低危漏洞 5 个。上述漏洞中，可利用来实施远程攻击的漏洞有 71 个。本周收录的漏洞中，已有 64 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“Cisco Prime Network Services Controller 任意命令执行漏洞”、“LOYTEC LIP-3ECTB-100 LVIS-3E100LIP-ME201 devices 信息泄露漏洞”等零日漏洞，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、合作伙伴及个人报送了本周收录的全部 78 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 1086 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)	680	680
安天实验室	103	1
启明星辰	77	0
恒安嘉新	55	0

绿盟科技	24	0
H3C	2	0
乌云	383	383
CNCERT 宁夏分中心	2	2
CNCERT 上海分中心	1	1
CNCERT 江西分中心	1	1
个人	18	18
报送总计	1346	1086
录入总计	78（去重）	1086

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Adobe、Samba、IBM 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	Adobe	9	12%
2	Samba	7	9%
3	IBM	5	6%
4	Linux	5	6%
5	PHP	4	5%
6	ASUS	4	5%
7	Cisco	4	5%
8	WordPress	3	4%
9	Samsung	3	4%
10	其他	34	44%

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 78 个漏洞。其中应用程序漏洞 49 个，网络设备漏洞 15 个，Web 应用漏洞 7 个，操作系统漏洞 5 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	49
网络设备漏洞	15
Web 应用漏洞	7
操作系统漏洞	5
安全产品漏洞	2

表 3 漏洞按影响类型统计表

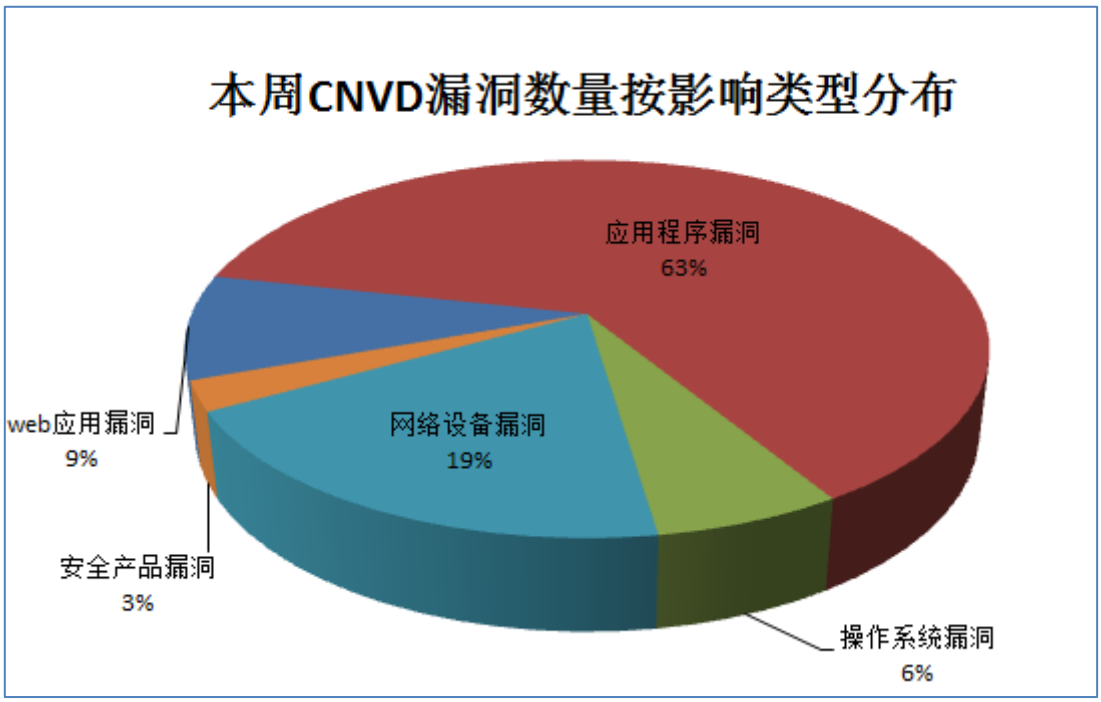

图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 10 个电信行业漏洞（如下图表所示）。其中，“Corega CG-WLBARAGM devices 拒绝服务漏洞”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-2015-08489	Cisco DPQ3925 devices with EDVA r1 Base 信息泄露漏洞	中	是
电信	CNVD-2015-08492	LOYTEC LIP-3ECTB-100 LVIS-3E100LIP-ME201 devices 信息泄露漏洞	高	否
电信	CNVD-2015-08526	WL-330NUL 信息泄露漏洞	低	是
电信	CNVD-2015-08527	WL-330NUL 远程命令执行漏洞	中	是
电信	CNVD-2015-08529	WL-330NUL 跨站脚本漏洞	中	是
电信	CNVD-2015-08528	WL-330NUL 拒绝服务漏洞	低	是
电信	CNVD-2015-08530	Corega CG-WLBARAGM devices 拒绝服务漏洞	高	是

电信	CNVD-2015-08532	ZTE ZXHN H108N R1A devices 信息泄露漏洞	中	是
电信	CNVD-2015-08539	Samsung Galaxy S6 拒绝服务漏洞	中	否
电信	CNVD-2015-08538	Samsung Galaxy S6 拒绝服务漏洞（CNVD-2015-085380）	中	否

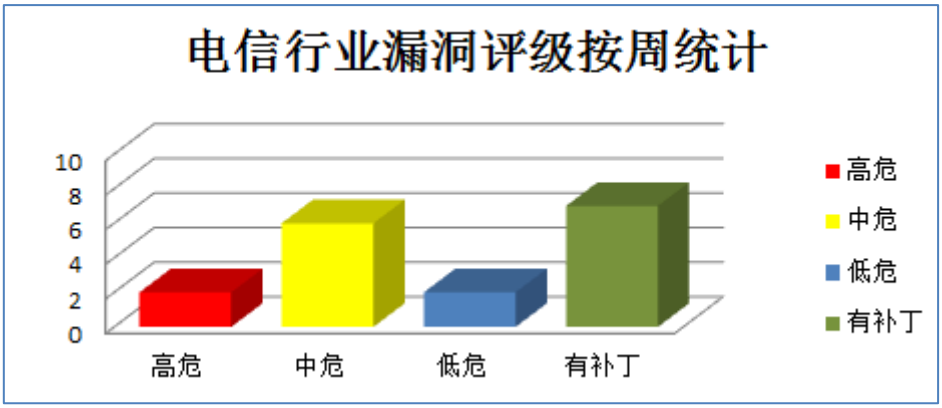

图 1 电信行业漏洞统计

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、 Adobe 产品安全漏洞

Adobe Flash Player、Adobe AIR SDK 和 Adobe AIR SDK & Compiler 都是美国奥多比（Adobe）公司的产品。Adobe Flash Player 是一款多媒体播放器产品；Adobe AIR SDK 和 Adobe AIR SDK & Compiler 都是适用于 Adobe AIR（一个跨操作系统的运行时环境）的标准开发工具包。本周，上述产品被披露存在内存错误引用、内存破坏和整数溢出漏洞。攻击者利用漏洞可执行任意代码。

CNVD 收录的相关漏洞包括：多款 Adobe 产品内存破坏漏洞（CNVD-2015-08515、CNVD-2015-08513）、多款 Adobe 产品内存错误引用漏洞（CNVD-2015-08512、CNVD-2015-08510、CNVD-2015-08509、CNVD-2015-08508、CNVD-2015-08507）、多款 Adobe 产品整数溢出漏洞（CNVD-2015-08511）。上述漏洞的综合评级均为“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-2015-08515

http://www.cnvd.org.cn/flaw/show/CNVD-2015-08513

http://www.cnvd.org.cn/flaw/show/CNVD-2015-08512

http://www.cnvd.org.cn/flaw/show/CNVD-2015-08510

http://www.cnvd.org.cn/flaw/show/CNVD-2015-08509

http://www.cnvd.org.cn/flaw/show/CNVD-2015-08508

http://www.cnvd.org.cn/flaw/show/CNVD-2015-08507

http://www.cnvd.org.cn/flaw/show/CNVD-2015-08511

2、 Samba 产品安全漏洞

Samba 是一套实现 SMB（Server Messages Block）协议、跨平台进行文件共享和打印共享服务的程序。本周，上述产品被披露存在信息泄露、访问绕过、中间人攻击和拒绝服务漏洞。攻击者利用上述漏洞可获取敏感信息、绕过访问限制和发起拒绝服务攻击等。

CNVD 收录的相关漏洞包括：Samba 拒绝服务漏洞、Samba 拒绝服务漏洞（CNVD-2015-08517、CNVD-2015-08524）、Samba 绕过访问权限漏洞（CNVD-2015-08520）、Samba 中间人攻击漏洞、Samba 绕过访问权限漏洞、Samba 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-2015-08517

http://www.cnvd.org.cn/flaw/show/CNVD-2015-08524

http://www.cnvd.org.cn/flaw/show/CNVD-2015-08520

http://www.cnvd.org.cn/flaw/show/CNVD-2015-08521

http://www.cnvd.org.cn/flaw/show/CNVD-2015-08522

http://www.cnvd.org.cn/flaw/show/CNVD-2015-08523

http://www.cnvd.org.cn/flaw/show/CNVD-2015-08525

3、 Linux 产品安全漏洞

Linux kernel 是美国 Linux 基金会发布的操作系统 Linux 所使用的内核。本周，上述产品被披露存在信息泄露、权限提升和拒绝服务漏洞。攻击者利用漏洞可获得敏感信息、提升权限和发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Linux kernel 拒绝服务漏洞（CNVD-2015-08552）、Linux kernel networking 拒绝服务漏洞、Linux Kernel ‘btrfs/inode.c’信息泄露漏洞、Linux kernel 本地提权漏洞（CNVD-2015-08501）、Linux kernel ‘fs/overlayfs/inode.c’本地提权漏洞。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-2015-08552

http://www.cnvd.org.cn/flaw/show/CNVD-2015-08551

http://www.cnvd.org.cn/flaw/show/CNVD-2015-08499

http://www.cnvd.org.cn/flaw/show/CNVD-2015-08501

http://www.cnvd.org.cn/flaw/show/CNVD-2015-08500

4、 IBM 产品安全漏洞

IBM Sterling B2B Integrator 是一套集成了重要的 B2B 流程、交易和关系的软件。IBM OpenPages GRC Platform 是美国 IBM 公司的一套用于管理企业风险和合规性挑战的治理、风险和合规性平台。该平台提供一组涵盖风险和合规性领域（包括操作风险、策略和合规性、财务控制管理的等）的核心服务和功能组件。IBM MQ Light 是美国 IBM 公司的一个基于 IBM Bluemix（在云上创建、部署和管理应用程序的 PaaS 平台）的消息服务。IBM B2B Advanced Communication 是美国 IBM 公司的一款通信网关产品。本周，上述产品被披露存在信息泄露、SQL 注入、安全绕过和拒绝服务漏洞。攻击者利用漏洞可获得敏感信息、绕过安全限制和发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：IBM Sterling B2B Integrator 安全绕过漏洞、IBM OpenPages GRC Platform SQL 注入漏洞、IBM MQ Light 拒绝服务漏洞、IBM MQ Light 远程拒绝服务漏洞、IBM B2B Advanced Communications 信息泄露漏洞。其中，“IBM OpenPages GRC Platform SQL 注入漏洞”的综合评级为“高”危。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-2015-08561

http://www.cnvd.org.cn/flaw/show/CNVD-2015-08556

http://www.cnvd.org.cn/flaw/show/CNVD-2015-08555

http://www.cnvd.org.cn/flaw/show/CNVD-2015-08554

http://www.cnvd.org.cn/flaw/show/CNVD-2015-08553

5、Cisco Prime Network Services Controller 任意命令执行漏洞

Cisco Prime Network Services Controller 是美国思科（Cisco）公司的一套云自动化网络管理软件。本周，Cisco Prime Network Services Controller 被披露存在任意命令执行漏洞。攻击者可利用该漏洞执行任意命令。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-2015-08487

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-2015-08485	PHP Intl 扩展存在拒绝服务漏洞	高	厂商已修复了该漏洞，请到厂商主页更新下载：http://www.php.net/
CNVD-2015-08486	Cacti SQL 注入漏洞（CNVD-2015-08486）	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://seclists.org/fulldisclosure/2015/Dec/8

CNVD-2015-08491	VMware vRealize Orchestrator 任意命令执行漏洞	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：http://www.vmware.com/security/advisories/VMSA-2015-0009.html
CNVD-2015-08503	PHP 远程格式化字符串漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：http://www.php.net/
CNVD-2015-08505	Google Chrome MIDI 子系统应用崩溃漏洞	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://googlechromereleases.blogspot.com/2015/12/stable-channel-update_15.html
CNVD-2015-08530	Corega CG-WLBARAGM devices 拒绝服务漏洞	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://jvndb.jvn.jp/en/contents/2015/JVNDB-2015-000201.html
CNVD-2015-08546	PHP 'ext/standard/string.c'任意代码执行漏洞	高	用户可联系供应商获得补丁信息：http://php.net/
CNVD-2015-08548	WordPress 插件 Pinpoint Booking System SQL 注入漏洞	高	用户可联系供应商获得补丁信息：http://wordpressbooking.systems/
CNVD-2015-08558	Blueman 远程提权漏洞	高	用户可联系供应商获得补丁信息：https://github.com/blueman-project/blueman
CNVD-2015-08560	PHP 'DateInterval'对象任意代码执行漏洞	高	用户可联系供应商获得补丁信息：http://php.net/

表 3 部分高危漏洞列表

小结：本周，多款 Adobe 产品被披露存在内存错误引用、内存破坏和整数溢出漏洞。攻击者利用漏洞可执行任意代码。此外，Samba、Linux、IBM 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、提升权限、执行任意代码和发起拒绝服务攻击等。另外，Cisco Prime Network Services Controller 被披露存在一个高危漏洞，攻击者可利用该漏洞执行任意命令。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、Google 修补 Chrome 产品漏洞

Google Chrome 是由 Google 开发的一款 Web 浏览工具。

本周，Google 修补了上述产品存在的系统应用崩溃漏洞，避免攻击者利用漏洞执行

任意代码和发起拒绝服务攻击。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网络安全事件。

补丁下载链接：http://www.cnvd.org.cn/patchInfo/show/69074

本周要闻速递

1. 欧洲信用卡终端机仍存在严重漏洞

德国研究人员在 Chaos Communication Congress（混乱通信大会）中介绍了现在欧洲的支付终端存在的一系列漏洞和拙劣的设计选项（该终端要求用户在输入四位 PIN 密码前先插入信用卡）。这些将允许黑客窃取受害者的 PIN 码和信用卡的磁条，黑客甚至可以伪装成任何终端设备并把资金转入任何一个德国的银行账户。这些无疑会引起欧洲其他国家体系的担忧，因为这些漏洞完全有可能也在其他国家的终端设备中存在。

参考链接：http://www.freebuf.com/news/91461.html

2. Android 恶意软件使用内置防火墙屏蔽安全软件

最近安全研究人员们发现他们现在使用开源的 Android 防火墙屏蔽安全软件与云服务器的通信。虽然这些恶意软件没有造成全球范围的影响，但不得不承认这样的新方法还是很有创意的。赛门铁克发现的最新案例是针对中国 Android 用户的一款恶意软件，赛门铁克将其命名为 Android.Spywaller。这个恶意软件的独特之处在于，感染目标设备后，它会查找奇虎 360 使用的 UID(唯一标识符, unique identifier)，之后它会加载 DroidWall 程序，这是 Android 平台上一款强大的防火墙前端软件，由 UNIX iptable 包修改而来。DroidWall 可以屏蔽安全软件连接云端检测服务器，导致安全软件变成鸡肋。

参考链接：http://www.freebuf.com/news/91563.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