

信息安全漏洞周报

2015 年 11 月 16 日-2015 年 11 月 22 日

2015 年第 47 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 133 个，其中高危漏洞 79 个、中危漏洞 42 个、低危漏洞 12 个。上述漏洞中，可利用来实施远程攻击的漏洞有 114 个。本周收录的漏洞中，已有 124 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“libsniff 堆缓冲区溢出漏洞”等零日代码攻击，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 133 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、绿盟科技等单位报送数量较多。补天平台、乌云、漏洞盒子、High-Tech Bridge Security Research Lab、习科网络安全及白帽子向 CNVD 提交了 945 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)	811	811
安天实验室	178	0
启明星辰	87	0
绿盟科技	70	0
天融信	67	0
恒安嘉新	60	0

H3C	2	0
High-Tech Bridge Security Research Lab	1	1
乌云	104	104
漏洞盒子	7	7
习科网络安全	1	1
CNCERT 山西分中心	5	5
CNCERT 宁夏分中心	1	1
个人	15	15
报送总计	1409	945
录入总计	133（去重）	945

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Microsoft、Adobe、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	Microsoft	45	34%
2	Adobe	16	12%
3	Cisco	5	4%
4	ZTE	5	4%
5	IBM	5	4%
6	FFmpeg	4	3%
7	Drupal	4	3%
8	Google	3	2%
9	Symantec	3	2%
10	其他	43	32%

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 91 个，操作系统漏洞 17 个，

网络设备漏洞 13 个，Web 应用漏洞 9 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	91
操作系统漏洞	17
网络设备漏洞	13
Web 应用漏洞	9
安全产品漏洞	3

表 3 漏洞按影响类型统计表

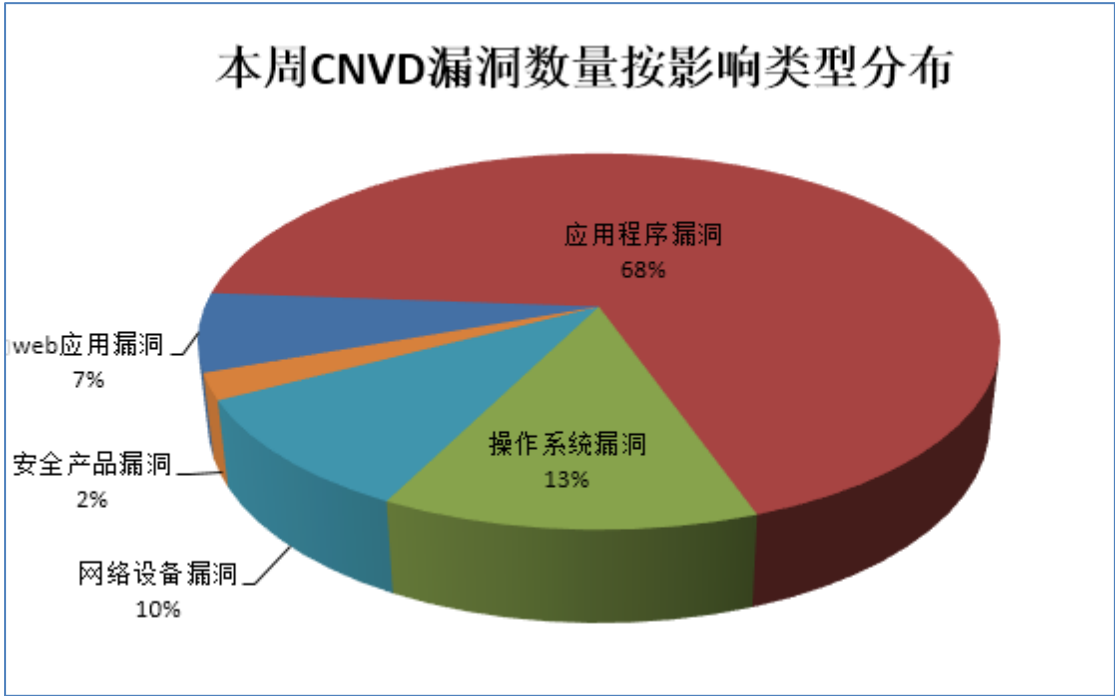


图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 9 个电信行业漏洞、1 个移动互联网行业漏洞、3 个工控系统行业漏洞（如下图表所示）。其中，“Lenovo Switch Center 竞争条件漏洞、IBM System Networking Switch Center 争用条件漏洞、ZTE ZXHN H108N R1A 默认账户权限绕过漏洞、ZTE ZXHN H108N R1A 任意文件读取漏洞、ZTE ZXHN H108N R1A 权限绕过漏洞、Samsung Galaxy S6 Edge 内存破坏漏洞、UnitronicsVisiLogic OPLC IDE 代码注入漏洞”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-2015-07564	Lenovo Switch Center 竞争条件漏洞	高	是
电信	CNVD-2015-07584	IBM System Networking Switch Center 争用条件漏洞	高	是
电信	CNVD-2015-07627	ZTE ZXHN H108N R1A webproccgi 模	低	是

		块跨站脚本漏洞		
电信	CNVD-2015-07626	ZTE ZXHN H108N R1A 默认账户权限绕过漏洞	高	是
电信	CNVD-2015-07625	ZTE ZXHN H108N R1A 任意文件读取漏洞	高	是
电信	CNVD-2015-07624	ZTE ZXHN H108N R1A 权限绕过漏洞	高	是
电信	CNVD-2015-07623	ZTE ZXHN H108N R1A 信息泄露漏洞	中	是
电信	CNVD-2015-07655	Samsung Galaxy S6 Edge 内存破坏漏洞	高	是
电信	CNVD-2015-07693	多款 GE 交换机跨站脚本漏洞	中	是
移动互联网	CNVD-2015-07579	BlackBerry Enterprise Server 跨站脚本漏洞	中	是
工控系统	CNVD-2015-07635	UnitronicsVisiLogic OPLC IDE 任意代码执行漏洞	中	是
工控系统	CNVD-2015-07636	UnitronicsVisiLogic OPLC IDE 代码注入漏洞	高	是
工控系统	CNVD-2015-07683	Exemys Telemetry Web Server 认证绕过漏洞	高	否

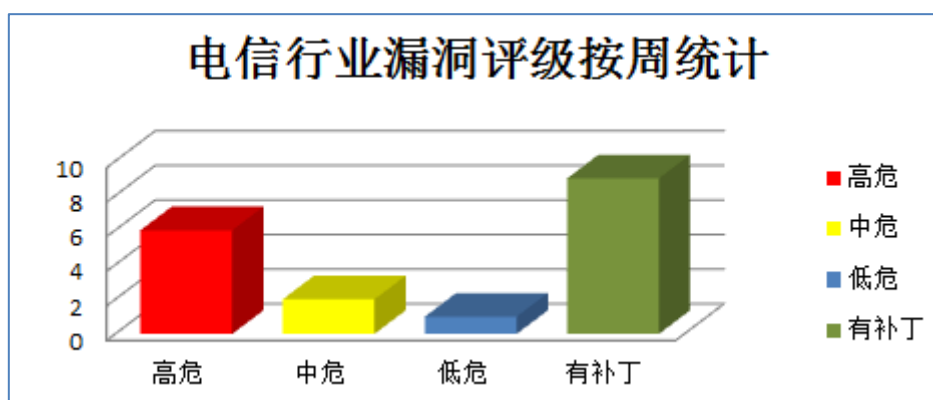


图 1 电信行业漏洞统计

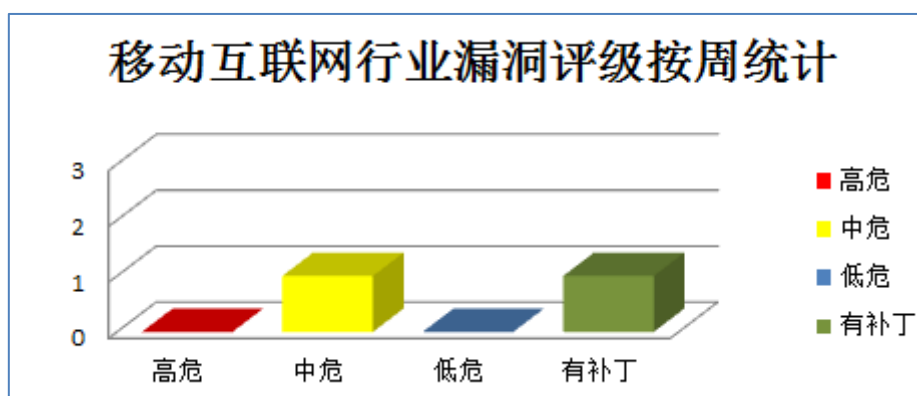


图 2 移动互联网行业漏洞统计

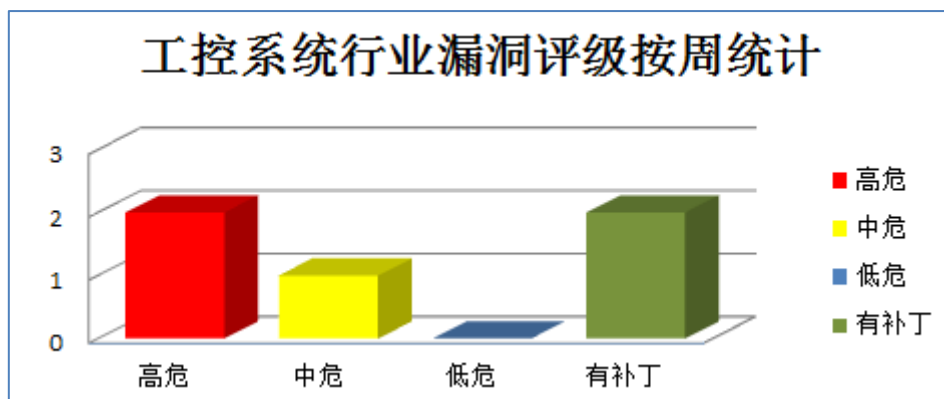


图3 工控系统行业漏洞统计

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、Redis 产品安全漏洞

近日，CNVD 收录了 Redis 未授权访问漏洞（CNVD-2015-07557）。远程攻击者利用漏洞，在未授权情况下可利用 Redis 的相关方法写入公钥，进而可以直接取得目标服务器管理权，发起进一步攻击。

CNVD 收录的相关漏洞包括：Redis 未授权访问漏洞。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-2015-07557>

2、Microsoft 产品安全漏洞

Microsoft Internet Explorer（IE）是美国微软（Microsoft）公司开发的一款 Web 浏览器，是 Windows 操作系统附带的默认浏览器。本周，上述产品被披露存在内存破坏漏洞。攻击者利用漏洞可执行任意代码。

CNVD 收录的相关漏洞包括：Microsoft Internet Explorer 内存破坏漏洞（CNVD-2015-07633、CNVD-2015-07580、CNVD-2015-07551、CNVD-2015-07535、CNVD-2015-07534、CNVD-2015-07550、CNVD-2015-07539、CNVD-2015-07538）。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-2015-07663>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-07580>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-07551>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-07535>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-07534>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-07550>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-07539>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-07538>

3、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漏洞。攻击者利用漏洞可执行任代码。

CNVD 收录的相关漏洞包括：Adobe Flash Player & Compiler 内存错误引用漏洞（CNVD-2015-07604、CNVD-2015-07603、CNVD-2015-07605、CNVD-2015-07607、CNVD-2015-07606、CNVD-2015-07610、CNVD-2015-07611、CNVD-2015-07608）。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-2015-07604>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-07603>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-07605>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-07607>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-07606>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-07610>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-07611>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-07608>

4、ZTE 产品安全漏洞

ZTE ZXHN H108N R1A 是中国中兴通讯公司的一款无线路由器产品。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、执行未授权操作等。

CNVD 收录的相关漏洞包括：ZTE ZXHN H108N R1A 信息泄露漏洞、ZTE ZXHN H108N R1A webproccgi 模块跨站脚本漏洞、ZTE ZXHN H108N R1A 默认账户权限绕过漏洞、ZTE ZXHN H108N R1A 任意文件读取漏洞、ZTE ZXHN H108N R1A 权限绕过漏洞。除“ZTE ZXHN H108N R1A 信息泄露漏洞、ZTE ZXHN H108N R1A webproccgi 模块跨站脚本漏洞”外，其余漏洞的综合评级为“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-2015-07623>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-07627>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-07626>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-07625>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-07624>

5、Symantec Endpoint Protection-RU6-MP3 不受信任搜索路径漏洞

Symantec Endpoint Protection 是赛门铁克开发的新一代企业级防病毒软件。本周，Symantec Endpoint Protection-RU6-MP3 被披露存在不受信任搜索路径漏洞。攻击者利用该漏洞可获得权限。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-2015-07565>

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-2015-07584	IBM System Networking Switch Center 争用条件漏洞	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://support.lenovo.com/us/en/product_security/len_2015_074
CNVD-2015-07578	IBM WebSphere Portal 内存消耗拒绝服务漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞： https://www-304.ibm.com/support/docview.wss?uid=swg21969906
CNVD-2015-07587	Google Chrome (Andriod) Javascript 处理任意代码执行漏洞	高	暂无
CNVD-2015-07602	Adobe Flash Player & Compiler 安全机制绕过漏洞	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://helpx.adobe.com/security/products/flash-player/apsb15-28.html
CNVD-2015-07601	Adobe Flash Player & Compiler 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://helpx.adobe.com/security/products/flash-player/apsb15-28.html
CNVD-2015-07617	IBM PowerHASystemMirror on AIX 超级用户权限提升漏洞	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-01.ibm.com/support/docview.wss?uid=isg1IV77007
CNVD-2015-07628	Google Chrome 同源策略绕过漏洞 (CNVD-2015-07628)	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://codereview.chromium.org/1316803003
CNVD-2015-07629	Schneider Electric IMT25 Magnetic Flow DTM for the HART Protocol 缓冲区溢出漏洞	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://download.schneider-electric.co

			m/files?p_Doc_Ref=SEVD-2015-215-01
CNVD-2015-07634	MIT Kerberos 5 缓冲区溢出漏洞	高	用户可参考如下供应商提供的安全公告获得补丁信息： https://github.com/krb5/krb5/commit/3db8dfec1ef50ddd78d6ba9503185995876a39fd
CNVD-2015-07665	FFmpeg 'init_tile'函数拒绝服务漏洞	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.ffmpeg.org/

表 3 部分高危漏洞列表

小结：本周，CNVD 收入了 Redis 未授权访问漏洞（CNVD-2015-07557）。远程攻击者利用漏洞，在未授权情况下可利用 Redis 的相关方法写入公钥，进而可以直接取得目标服务器管理权，发起进一步攻击。此外，Microsoft、Adobe、ZTE 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、进行未授权访问和执行任意代码等。另外，Symantec Endpoint Protection-RU6-MP3 被披露存在一个高危漏洞，攻击者利用该漏洞可获取权限。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 ArcSight Management Center 和 ArcSight Logger 产品漏洞

HP ArcSight Management Center 是美国惠普（HP）公司的安全管理中心。HP ArcSight Logger 是一款日志管理软件工具。

本周，HP 修补了上述产品存在的跨站脚本漏洞，避免将用户重定向到任意网站，并进行钓鱼攻击。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/66827>

本周要闻速递

1. PNG 图片处理库 libpng 曝出漏洞

据报道：图片处理库 libpng 日前曝出漏洞。目前，该漏洞仅能造成拒绝服务，但其后续影响绝不可能仅限于此。因为这项漏洞还允许恶意攻击者造成应用程序崩溃，而这正是恶意攻击者们实现进一步入侵的最佳选择的起点。目前 libpng 的 1.6.19、1.5.24、1.4.17、1.2.54 以及 1.0.64 等版本已经于 2015 年 11 月 12 号获得了最新修复。

参考链接: <http://www.freebuf.com/news/86074.html>

2. VMware 更新、修复 Apache Flex BlazeDS 中的漏洞

VMware 发布了数个产品的版本更新, 目的是修复 Apache Flex BlazeDS 中的一个漏洞。据 VMware 介绍, Flex BlazeDS 组件应用在数个公司产品中, 但是其上存在 XML 外部实体 (XXE) 漏洞, 可被攻击者远程利用, 发送一条特制的 XML 请求, 服务器便会泄露信息。该漏洞对 VMware vCenter Server 5.0、5.1、5.5, vCloud Director 5.5、5.6, Horizon View 5.0、6.0 均有影响。但随着 VMware vCenter Server 5.0u3e、5.1u3b、5.5u3, vCloud Director 5.5.3、5.6.4, Horizon View 5.3.4、6.1 新版本的更新, 问题已被解决。vCenter Server 6.0 不受影响。

参考链接: <http://www.freebuf.com/news/86423.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