国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2017 年 12 月 18 日-2017 年 12 月 24 日 **2017 年第 52 期**

本周漏洞态势研判情况

本周信息安全漏洞威胁整体评价级别为**高**。

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 440 个，其中高危漏洞 194 个、中危漏洞 202 个、低危漏洞 44 个。漏洞平均分值为 6.06 本周收录的漏洞中，涉及 0day 漏洞 142 个（占 32%），其中互联网上出现“PHICOMM K2（PSG1218）输入验证漏洞、Debut embedded http server 拒绝服务漏洞”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 466 个，与上周（567 个）环比减少 18%。

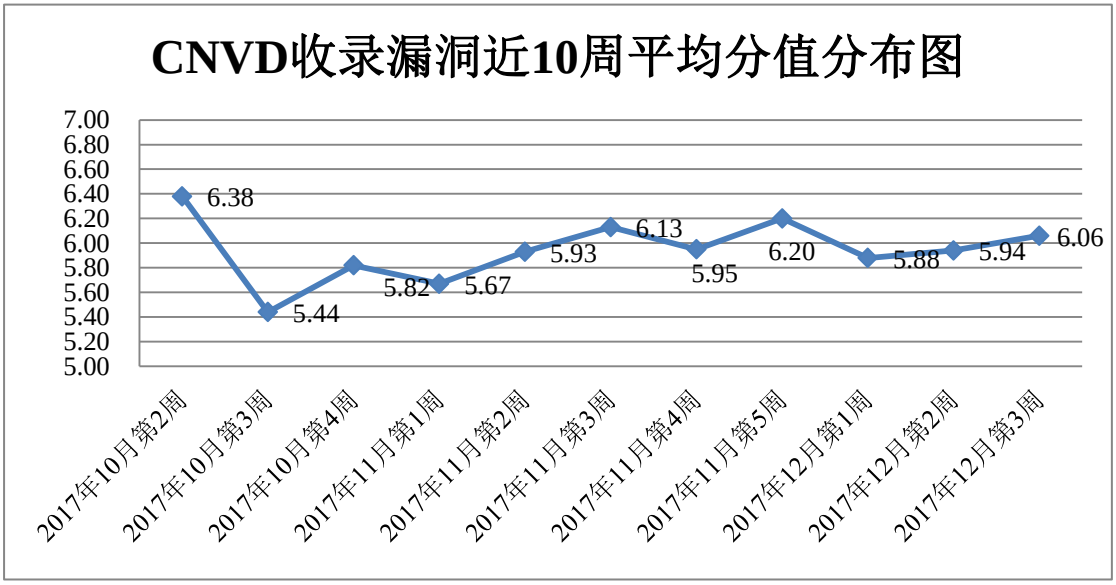

图 1 CNVD 收录漏洞近 10 周平均分值分布图

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，东软、华为技术有限公司、H3C、安天实验室、恒安嘉新等单位报送数量较多。南京联成科技发展股份有限公司、成都思维世纪科技有限公司、中新网络信息安全股份有限公司、四川虹微技术有限公司（子午攻防实验室）、

上海观安信息技术股份有限公司、漏斗社区、福建省海峡信息技术有限公司、君立华域、深圳盒子支付信息技术有限公司、北京智游网安科技有限公司及其他个人白帽子向 CNVD 提交了 466 个以事件型漏洞为主的原创漏洞。

表 1 漏洞报送情况统计表

报送单位或个人	漏洞报送数量	原创漏洞数量
东软	422	0
华为技术有限公司	257	0
H3C	186	0
安天实验室	181	0
恒安嘉新	162	0
网神	148	148
绿盟科技	118	0
中国电信集团系统集成有限责任公司	96	0
启明星辰	93	0
天融信	83	5
杭州安恒信息技术有限公司	53	2
漏洞盒子	22	22
卫士通信息产业股份有限公司	2	0
知道创宇	1	0
南京联成科技发展股份有限公司	23	23
成都思维世纪科技有限公司	8	8
中新网络信息安全股份有限公司	8	8
四川虹微技术有限公司（子午攻防实验室）	6	6
上海观安信息技术股份有限公司	4	4

漏斗社区	2	2
福建省海峡信息技术有限公司	1	1
君立华域	1	1
深圳盒子支付信息技术有限公司	1	1
北京智游网安科技有限公司	1	1
CNCERT 重庆分中心	5	5
CNCERT 广东分中心	4	4
CNCERT 新疆分中心	4	4
CNCERT 浙江分中心	2	2
CNCERT 陕西分中心	1	1
个人	218	218
报送总计	2113	466

本周漏洞按类型和厂商统计

本周，CNVD 收录了 440 个漏洞。其中应用程序漏洞 296 个，web 应用漏洞 60 个，网络设备漏洞 60 个，操作系统漏洞 18 个，安全产品漏洞 4 个，数据库漏洞 2 个。

表 2 漏洞按影响类型统计表

漏洞影响对象类型	漏洞数量
应用程序漏洞	296
web 应用漏洞	60
网络设备漏洞	60
操作系统漏洞	18
安全产品漏洞	4
数据库漏洞	2

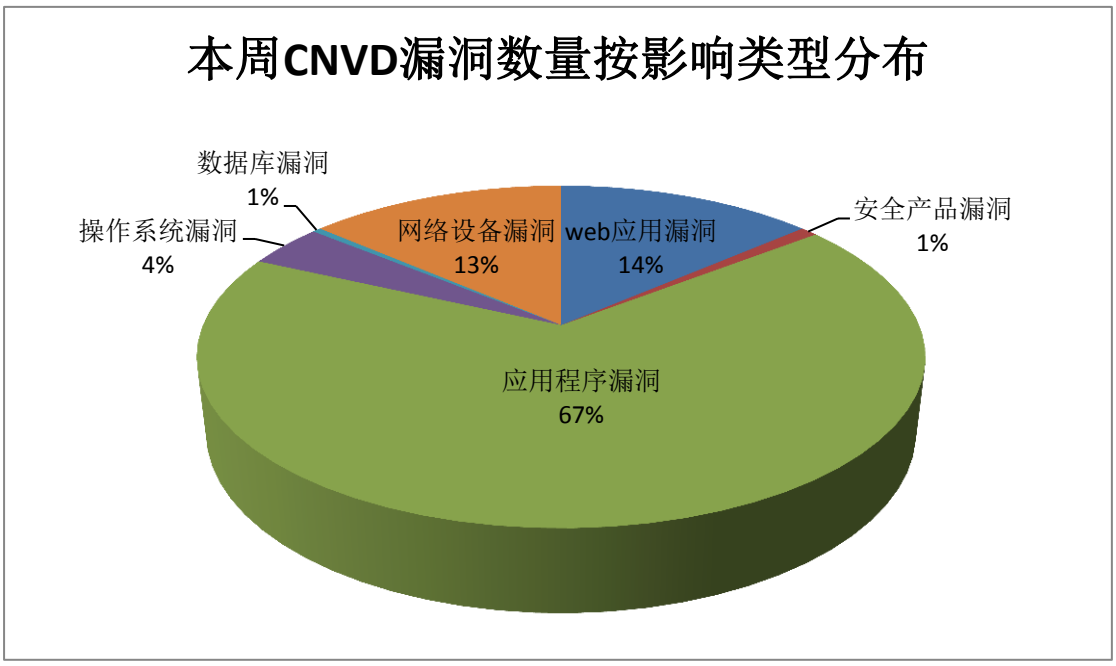

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 IBM、PHP Scripts Mall、Huawei 等多家厂商的产品，部分漏洞数量按厂商统计如表 3 所示。

表 3 漏洞产品涉及厂商分布统计表

序号	厂商（产品）	漏洞数量	所占比例
1	IBM	43	10%
2	PHP Scripts Mall	43	10%
3	Huawei	30	7%
4	Quest	22	5%
5	FS	21	5%
6	Intel	10	2%
7	QNAP	9	2%
8	VMware	7	2%
9	WordPress	7	2%
10	其他	248	55%

本周行业漏洞收录情况

本周，CNVD 收录了 34 个电信行业漏洞，11 个移动互联网行业漏洞，6 个工控行业漏洞（如下图所示）。其中，“Vonage VDV-23 115 拒绝服务漏洞、多款 Huawei 产品输入校验漏洞、Google Android NVIDIA Thermal 驱动程序权限提升漏洞、WECON L

eviStudio HMI 堆缓冲区溢出漏洞、MOXA EDS-G512E 拒绝服务漏洞”等漏洞的综合评级为“高危”。相关厂商已经发布了上述漏洞的修补程序，请参照 CNVD 相关行业漏洞库链接。

电信行业漏洞链接：http://telecom.cnvd.org.cn/

移动互联网行业漏洞链接：http://mi.cnvd.org.cn/

工控系统行业漏洞链接：http://ics.cnvd.org.cn/

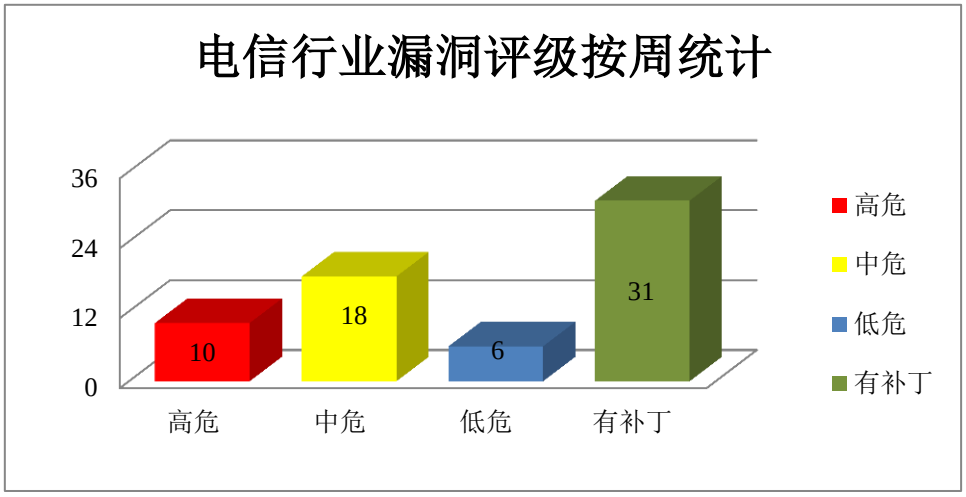

图 3 电信行业漏洞统计

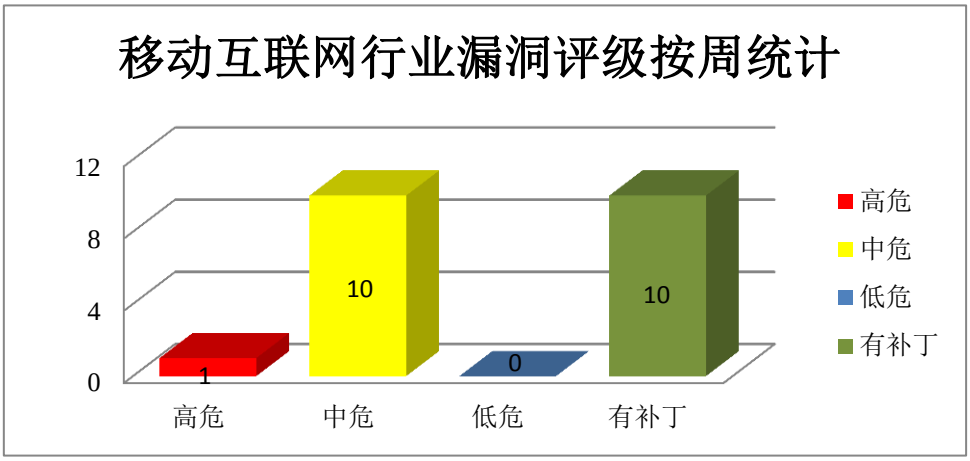

图 4 移动互联网行业漏洞统计

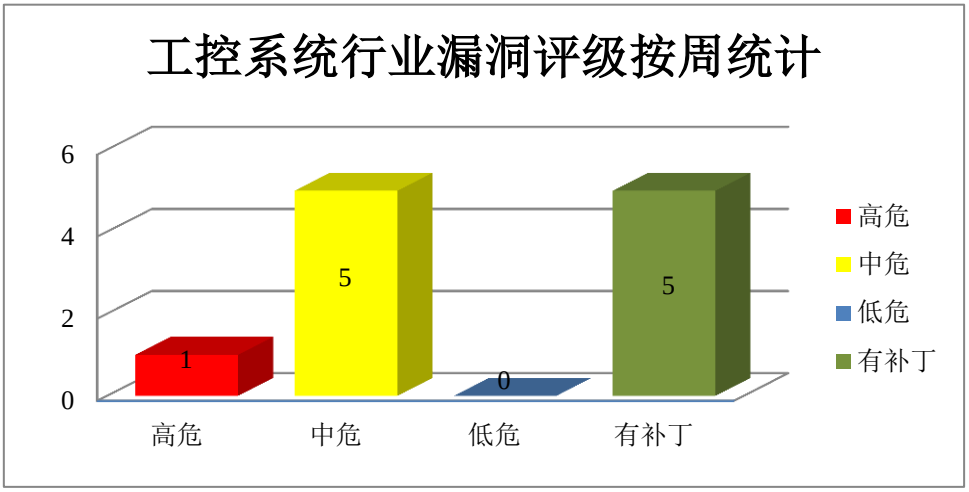

图 5 工控行业漏洞统计

本周重要漏洞安全告警

本周，CNVD 整理和发布以下重要安全漏洞信息。

1、IBM 产品安全漏洞

IBM Sterling File Gateway 是美国 IBM 公司的一套文件传输软件，IBM Atlas eDiscovery Process Management 是一款信息生命周期治理解决方案中的产品，IBM Tivoli Monitoring 是系统监控软件，IBM Jazz for Service Management 是一款提供对服务管理环境可见性的集成服务管理产品。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞获取数据库敏感信息、执行任意代码或绕过安全限制等。

CNVD 收录的相关漏洞包括：IBM Jazz for Service Management 跨站请求伪造漏洞（CNVD-2017-37857、CNVD-2017-37866）、IBM Atlas eDiscovery Process Management SQL 注入漏洞、IBM Financial Transaction Manager SQL 注入漏洞、IBM QRadar 命令注入漏洞、IBM Security Guardium Database Activity Monitor SQL 注入漏洞、IBM Sterling File Gateway 安全绕过漏洞、IBM Tivoli Monitoring 任意代码执行漏洞。除“IBM Jazz for Service Management 跨站请求伪造漏洞（CNVD-2017-37857、CNVD-2017-37866）”外，其余漏洞的综合评级为“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-2017-37857

http://www.cnvd.org.cn/flaw/show/CNVD-2017-37866

http://www.cnvd.org.cn/flaw/show/CNVD-2017-37592

http://www.cnvd.org.cn/flaw/show/CNVD-2017-37588

http://www.cnvd.org.cn/flaw/show/CNVD-2017-37867

http://www.cnvd.org.cn/flaw/show/CNVD-2017-37858

http://www.cnvd.org.cn/flaw/show/CNVD-2017-37582

http://www.cnvd.org.cn/flaw/show/CNVD-2017-37722

2、Huawei 产品安全漏洞

Huawei AR120-S 等都是中国华为（Huawei）公司的路由器产品，Huawei S12700 等是智能路由交换机。Huawei USG 系列产品及 Secospace USG 系列是新一代专业入侵防御和防火墙产品。Huawei 畅享 5S 是一款智能手机。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞读取数据、泄露内存信息或发起拒绝服务攻击等。

CNVD 收录的相关漏洞包括：多款 Huawei 产品 IPv6 协议越边界读取漏洞、多款 Huawei 产品输入校验漏洞、多款 Huawei 产品输入验证漏洞（CNVD-2017-37728）、多款 Huawei 防火墙产品存在内存泄露漏洞、多款 Huawei 路由器产品数值计算错误漏洞、多款 Huawei 产品拒绝服务漏洞（CNVD-2017-37724、CNVD-2017-37726）、Huawei 畅享 5S 信息泄露漏洞。除“多款 Huawei 产品拒绝服务漏洞（CNVD-2017-37726）、Huawei 畅享 5S 信息泄露漏洞”外，其余漏洞的综合评级为“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-2017-37845

http://www.cnvd.org.cn/flaw/show/CNVD-2017-37723

http://www.cnvd.org.cn/flaw/show/CNVD-2017-37728

http://www.cnvd.org.cn/flaw/show/CNVD-2017-37507

http://www.cnvd.org.cn/flaw/show/CNVD-2017-37844

http://www.cnvd.org.cn/flaw/show/CNVD-2017-37724

http://www.cnvd.org.cn/flaw/show/CNVD-2017-37726

http://www.cnvd.org.cn/flaw/show/CNVD-2017-37499

3、Quest 产品安全漏洞

Quest NetVault Backup 是美国 Quest Software 公司的一套数据备份软件。本周，该产品被披露存在 SQL 注入漏洞，攻击者可利用漏洞获取数据库敏感信息。

CNVD 收录的相关漏洞包括：Quest NetVault Backup SQL 注入漏洞（CNVD-2017-37630、CNVD-2017-37631、CNVD-2017-37632、CNVD-2017-37633、CNVD-2017-37634、CNVD-2017-37635、CNVD-2017-37636、CNVD-2017-37637）。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-2017-37630

http://www.cnvd.org.cn/flaw/show/CNVD-2017-37631

http://www.cnvd.org.cn/flaw/show/CNVD-2017-37632

http://www.cnvd.org.cn/flaw/show/CNVD-2017-37633

http://www.cnvd.org.cn/flaw/show/CNVD-2017-37634

http://www.cnvd.org.cn/flaw/show/CNVD-2017-37635

http://www.cnvd.org.cn/flaw/show/CNVD-2017-37636

http://www.cnvd.org.cn/flaw/show/CNVD-2017-37637

4、QNAP 产品安全漏洞

QNAP QTS 是中国威联通（QNAP Systems）公司的一套 Turbo NAS 作业系统。Video Station 是其中的一个视频播放器。本周，上述产品被披露存在缓冲区溢出和 SQL 注入漏洞，攻击者可利用漏洞执行任意代码或获取数据库敏感信息。

CNVD 收录的相关漏洞包括：QNAP QTS 缓冲区溢出漏洞、QNAP QTS 缓冲区溢出漏洞（CNVD-2017-37605、CNVD-2017-37606、CNVD-2017-37607、CNVD-2017-37608、CNVD-2017-37609、CNVD-2017-37610）、QNAP Video Station 命令注入漏洞。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-2017-37604

http://www.cnvd.org.cn/flaw/show/CNVD-2017-37605

http://www.cnvd.org.cn/flaw/show/CNVD-2017-37606

http://www.cnvd.org.cn/flaw/show/CNVD-2017-37607

http://www.cnvd.org.cn/flaw/show/CNVD-2017-37608

http://www.cnvd.org.cn/flaw/show/CNVD-2017-37609

http://www.cnvd.org.cn/flaw/show/CNVD-2017-37610

http://www.cnvd.org.cn/flaw/show/CNVD-2017-37603

5、多款 Shenzhen Tenda 产品 app_data_center 命令注入漏洞

Shenzhen Tenda Ac9 等都是中国腾达（Tenda）公司的无线路由器产品。本周，Tenda 被披露存在命令注入漏洞，远程攻击者可通过发送特制的 cgi-bin/luci/usbeject?dev_name= GET 请求利用该漏洞执行任意的操作系统命令。目前，厂商尚未发布漏洞修补程序。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_-2017-37811

更多高危漏洞如表 4 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-2017-37282	ldns 双重释放漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://git.nlnetlabs.nl/ldns/commit/?id=c8391790
CNVD-2017-37570	Xen 'Hypervisor'内存破坏漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://xenbits.xen.org/xsa/advisory-249

			.html
CNVD-2017-37577	Xen '/mm/hap/hap.c'内存破坏漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://xenbits.xen.org/xsa/advisory-248.html
CNVD-2017-37604	QNAP QTS 缓冲区溢出漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://www.qnap.com/en/security-advisory/nas-201712-15
CNVD-2017-37614	iBall iB-WRA300N3GT 权限提升漏洞	高	目前厂商已发布升级补丁以修复漏洞，详情请关注厂商主页：https://www.iball.co.in
CNVD-2017-37689	WECON LeviStudio HMI 堆缓冲区溢出漏洞	高	用户可联系供应商获得补丁信息：http://www.we-con.com.cn/en/download.aspx?id=45
CNVD-2017-37710	xrdp 'scp_v0s_accept'函数拒绝服务漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://github.com/neutrinolabs/xrdp/pull/958
CNVD-2017-37715	PCRE 本地堆栈缓冲区溢出漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：http://www.pcre.org/
CNVD-2017-37821	Ipsilon 存在未明漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://ipsilon-project.org/release/2.1.0.html
CNVD-2017-37822	Ikiwiki 提权漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://ikiwiki.info/security/#index46h2

表 4 部分重要高危漏洞列表

小结：本周，IBM 被披露存在多个漏洞，攻击者可利用漏洞获取数据库敏感信息、执行任意代码或绕过安全限制等。此外，Huawei、Quest、QNAP 等多款产品被披露存在多个漏洞，攻击者可利用漏洞获取数据库敏感信息、执行任意代码或发起拒绝服务攻击等。另外，Tenda 被披露存在命令注入漏洞，远程攻击者可通过发送特制的 cgi-bin/luci/usbeject?dev_name= GET 请求利用该漏洞执行任意的操作系统命令。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。

本周漏洞要闻速递

1. 美国电信运营商 AT&T 的 DirectTV WVB 设备被爆出 0day 远程 Root 漏洞

趋势科技安全研究人员 RickyLawshae 公开了 AT&T DirecTV WVB 设备组件中存

在易于利用的 0day 漏洞(编号 CVE-2017-17411)，黑客利用该漏洞可以获取 root 权限，从而完全控制该设备，数百万注册 DirecTV 服务的用户将面临风险。此次公布的漏洞问题在于 Genie DVR 系统的一个核心组件，该组件附带了免费的 DirecTV，这个很容易被黑客利用，从而获得 root 权限，并完全控制该设备。这个漏洞实际上存在于 Linksys 制造的 WVBR0-25，它是一款 Linux 驱动的无线视频桥。DirecTV 无线视频桥 WVBR0-25 允许 Genie DVR 与客户的 Genie 客户端(最多 8 个)空中对接，和家里的电视进行通信，A&A 向其新客户提供了这个平台。

参考链接：http://www.freebuf.com/news/157184.html

2. WebLogic XMLDecoder 反序列化漏洞

Oracle Fusion Middleware（Oracle 融合中间件）是美国甲骨文（Oracle）公司的一套面向企业和云环境的业务创新平台。该平台提供了中间件、软件集合等功能。Oracle WebLogic Server 是其中的一个适用于云环境和传统环境的应用服务器组件。Oracle Fusion Middleware 中的 Oracle WebLogic Server 组件的 WLS Security 子组件存在安全漏洞。使用精心构造的 xml 数据可能造成任意代码执行，攻击者只需要发送精心构造的 HTTP 请求，就可以拿到目标服务器的权限。攻击者可利用该漏洞控制组件，影响数据的可用性、保密性和完整性。

参考链接：http://www.freebuf.com/news/158007.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：010-82991537