国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2017 年 01 月 23 日-2017 年 02 月 05 日 **2017 年第5、6 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**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 170 个，其中高危漏洞 44 个、中危漏洞 104 个、低危漏洞 22 个。漏洞平均分值为 5.76。本周收录的漏洞中，涉及 0day 漏洞 11 个（占 7%）。其中互联网上出现“WordPress REST API 插件内容注入漏洞、Samsung Smartcam 命令注入漏洞、Microsoft Windows SMB TreeConnect 响应拒绝服务漏洞”等零日漏洞，请使用相关产品的用户注意加强防范。此外，本周，时值春节期间，CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 199 个，与上周单周（574 个）环比下降 65%。

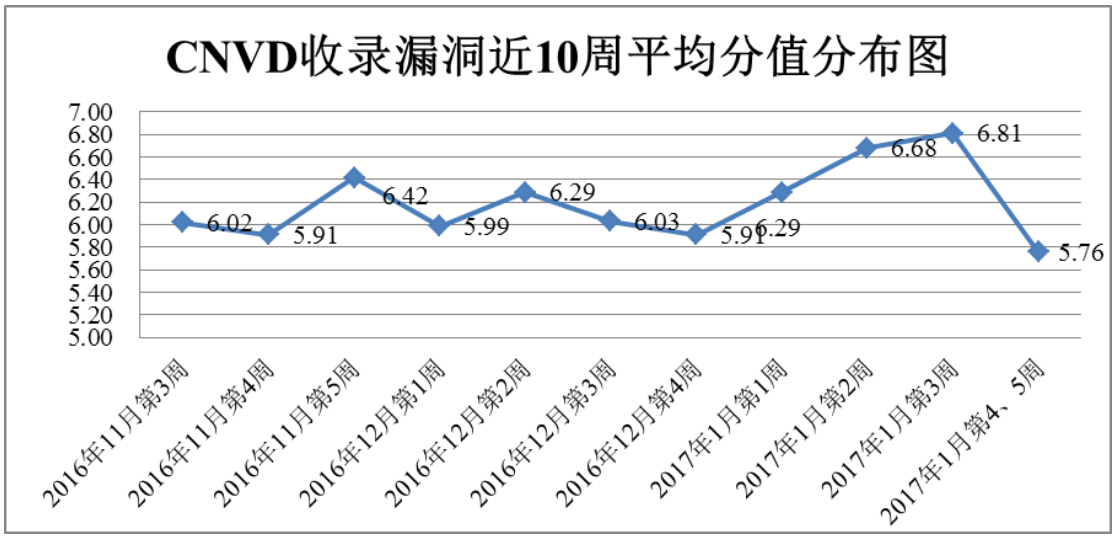

图 1 CNVD 收录漏洞近 10 周平均分值分布图

本周漏洞报送情况统计

本周，共 7 家成员单位、合作伙伴及企业用户、个人用户报送了本周收录的全部 170 个漏洞。报送情况如表 1 所示。其中，蓝盾信息安全技术股份有限公司、华为技术有限公司等单位报送数量较多。360 网神、漏洞盒子、新疆天山智汇信息科技有限公司及其

他个人白帽子向 CNVD 提交了 199 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
蓝盾信息安全技术股份有限公司	97	0
华为技术有限公司	92	0
360 网神	59	59
天融信	21	0
安全狗	12	0
北京数字观星科技有限公司	5	0
恒安嘉新	2	0
漏洞盒子	48	48
知道创宇	3	0
新疆天山智汇信息科技有限公司	1	1
CNCERT 江西分中心	24	24
CNCERT 山西分中心	13	13
CNCERT 湖南分中心	7	7
CNCERT 宁夏分中心	7	7
CNCERT 福建分中心	6	6
CNCERT 浙江分中心	3	3
CNCERT 新疆分中心	3	3
个人	28	28
报送总计	431	199
录入总计	170（去重）	199

表 1 漏洞报送情况统计表

本周漏洞按类型和厂商统计

本周，CNVD 收录了 170 个漏洞。其中应用程序漏洞 131 个，web 应用漏洞 19 个，操作系统漏洞 11 个，网络设备漏洞 6 个，数据库漏洞 3 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	131
web 应用漏洞	19
操作系统漏洞	11
网络设备漏洞	6
数据库漏洞	3

表 2 漏洞按影响类型统计表

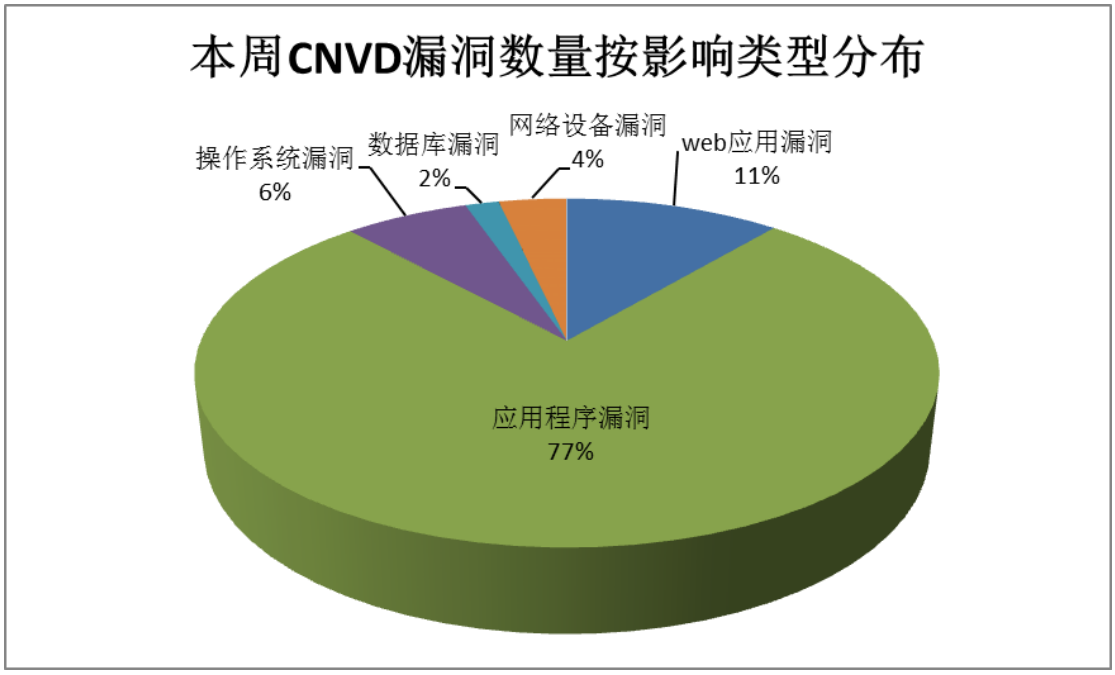

图 2 本周漏洞按影响类型分布

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

序号	厂商（产品）	漏洞数量	所占比例
1	Oracle	48	28%
2	Zimbra	16	9%
3	Cisco	9	5%
4	Linux	9	5%
5	MetalGenix	6	4%
6	Brocade	5	3%
7	Honeywell	5	3%
8	Micro Code	5	3%

9	IBM	4	2%
10	其他	63	38%

表 3 漏洞产品涉及厂商分布统计表

本周行业漏洞收录情况

本周，CNVD 收录了 6 个电信行业漏洞，3 个移动互联网行业漏洞，6 个工控系统行业漏洞（如下图所示）。其中，“Oracle WebLogic Server 远程安全漏洞、Honeywell XL Web II Controller 权限管理不当漏洞、Honeywell XL Web II Controller 会话固定漏洞、Honeywell XL Web II Controller 明文存储密码漏洞（CNVD-2017-00914）、Honeywell XL Web II Controller 明文存储密码漏洞、Honeywell XL Web II Controller 目录遍历漏洞”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/

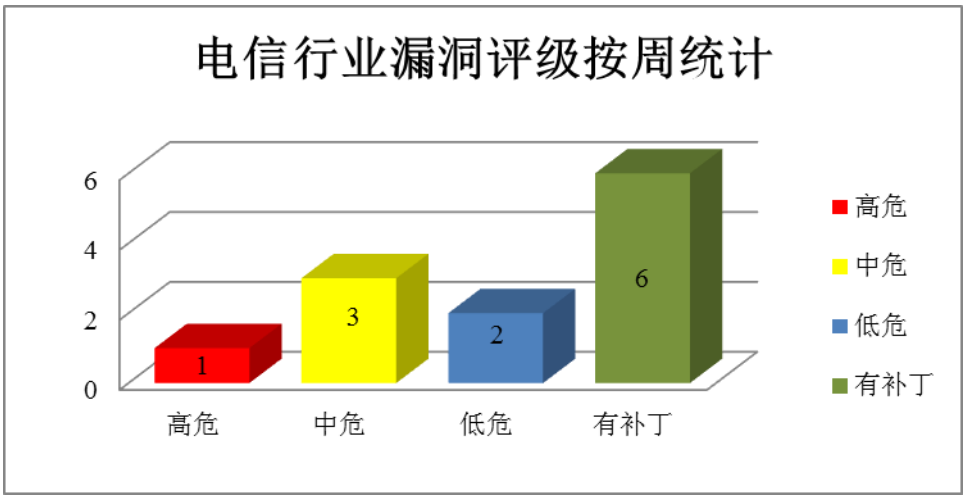

图 3 电信行业漏洞统计

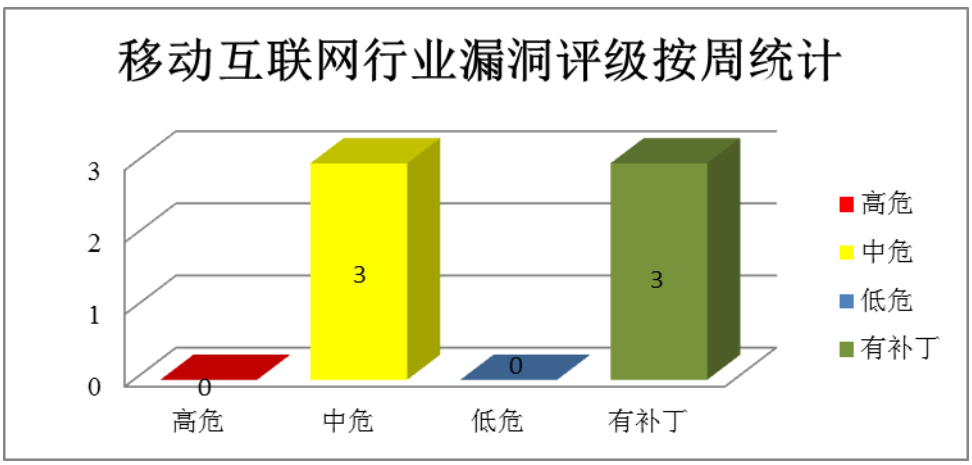

图 4 移动互联网行业漏洞统计

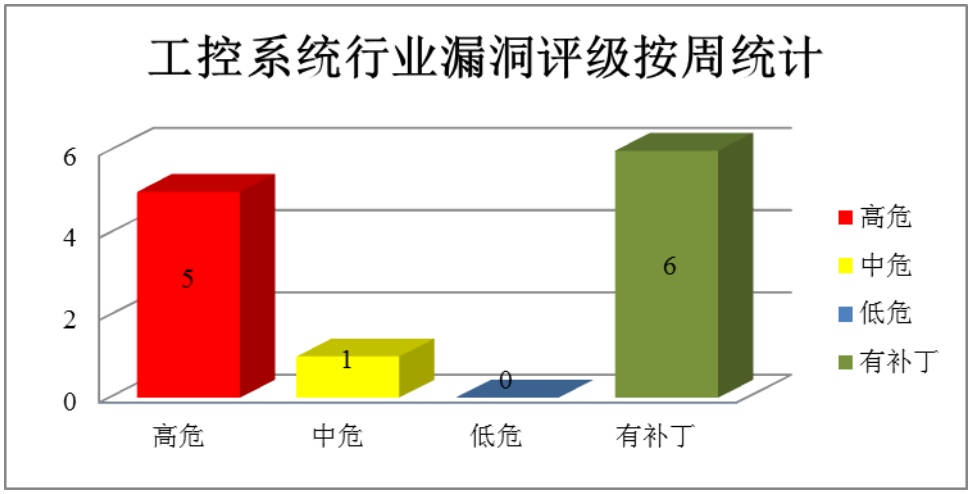

图 5 工控系统行业漏洞统计

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、Cisco WebEx 产品安全漏洞

Cisco WebEx 是浏览器扩展插件。本周，该产品被披露存在远程代码执行漏洞，攻击者可利用漏洞执行任意代码。

CNVD 收录的相关漏洞包括：Cisco WebEx 浏览器插件远程代码执行漏洞。该漏洞的综合评级为“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-2017-00743

2、Microsoft Windows 产品安全漏洞

Microsoft Windows 是美国微软公司发布的一系列操作系统。本周，该产品被披露存在拒绝服务漏洞，攻击者可利用漏洞发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Microsoft Windows SMB Tree Connect 响应拒绝服务漏洞，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-2017-00819

3、Oracle 产品安全漏洞

Oracle Primavera ProductsPrimavera Products Suite 是美国甲骨文（Oracle）公司的一款项目组合管理解决方案套件产品；Oracle FLEXCUBE Universal Banking 是一套实时的、在线覆盖零售、团体、投资银行业务的综合性解决方案；Oracle WebLogic Server 是一款适用于云环境和传统环境的应用服务器；Oracle GlassFish Server 是一套可实现 Java Platform、Java EE 6 规范的解决方案。本周，上述产品被披露存在多个漏洞，

攻击者可利用漏洞进行未授权访问、更新、插入或删除数据，影响数据的保密性、完整性和可用性。

CNVD 收录的相关漏洞包括：Oracle Primavera 产品远程漏洞、Oracle FLEXCUBE Private Banking 安全绕过漏洞（CNVD-2017-00791、CNVD-2017-00787）、Oracle FLEXCUBE Universal Banking 存在未明漏洞（CNVD-2017-00945、CNVD-2017-00944）、Oracle WebLogic Server 远程安全漏洞、Oracle GlassFish Server 远程安全漏洞（CNVD-2017-00928、CNVD-2017-00929）。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-2017-00908
http://www.cnvd.org.cn/flaw/show/CNVD-2017-00791
http://www.cnvd.org.cn/flaw/show/CNVD-2017-00787
http://www.cnvd.org.cn/flaw/show/CNVD-2017-00945
http://www.cnvd.org.cn/flaw/show/CNVD-2017-00944
http://www.cnvd.org.cn/flaw/show/CNVD-2017-00919
http://www.cnvd.org.cn/flaw/show/CNVD-2017-00928
http://www.cnvd.org.cn/flaw/show/CNVD-2017-00929

4、Honeywell 产品安全漏洞

Honeywell XL Web Controller 是基于 Web 的 SCADA 系统。本周，该产品被披露存在多个漏洞，攻击者可利用漏洞泄露敏感信息或发起路径遍历攻击等。

CNVD 收录的相关漏洞包括：Honeywell XL Web II Controller 权限管理不当漏洞、Honeywell XL Web II Controller 会话固定漏洞、Honeywell XL Web II Controller 明文存储密码漏洞（CNVD-2017-00914）、Honeywell XL Web II Controller 明文存储密码漏洞、Honeywell XL Web II Controller 目录遍历漏洞。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-2017-00912
http://www.cnvd.org.cn/flaw/show/CNVD-2017-00913
http://www.cnvd.org.cn/flaw/show/CNVD-2017-00914
http://www.cnvd.org.cn/flaw/show/CNVD-2017-00915
http://www.cnvd.org.cn/flaw/show/CNVD-2017-00916

5、Samsung Smartcam 命令注入漏洞

Samsung SmartCam 是基于云端服务的安全监控摄像头。本周，Samsung 被披露存在命令注入漏洞。攻击者可利用漏洞注入 shell 命令，获取 root 权限执行远程代码。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-2017-00815

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-2017-00703	Brocade Network Advisor 目录遍历漏洞	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：https://www.brocade.com/
CNVD-2017-00702	Brocade Network Advisor 目录遍历漏洞（CNVD-2017-00702）	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:https://www.brocade.com/
CNVD-2017-00701	Brocade Network Advisor 目录遍历漏洞（CNVD-2017-00701）	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:https://www.brocade.com/
CNVD-2017-00700	Brocade Network Advisor 目录遍历漏洞（CNVD-2017-00700）	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:https://www.brocade.com/
CNVD-2017-00732	Aerospike Database Server 缓冲区溢出漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：http://www.aerospike.com/
CNVD-2017-00746	Apache Groovy 远程代码执行漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：http://groovy-lang.org/security.html
CNVD-2017-00794	Citrix Provisioning Services 内存错误引用漏洞	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.citrix.com/article/CTX219580
CNVD-2017-00796	Citrix Provisioning Services 缓冲区溢出漏洞	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.citrix.com/article/CTX219580
CNVD-2017-00866	Artifex Software MuJS 整数溢出漏洞	高	用户可联系供应商获得补丁信息：http://mujs.com/
CNVD-2017-00924	Docker 本地权限提升漏洞（CNVD-2017-00924）	高	用户可联系供应商获得补丁信息：https://www.docker.com/

表 4 部分重要高危漏洞列表

小结：半轴 Cisco WebEx 被披露存在远程代码执行漏洞，攻击者可利用漏洞执行任

意代码。此外，Microsoft Windows、Oracle、Honeywell 等多款产品被披露存在多个漏洞，攻击者利用漏洞可执行任意代码、泄露敏感信息或发起拒绝服务攻击等。另外，Samsung 被披露存在命令注入漏洞。攻击者可利用漏洞注入 shell 命令，获取 root 权限执行远程代码。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。

本周漏洞要闻速递

1. 大量 Netgear 路由器存在密码绕过漏洞

Netgear 路由器遭遇一起严重安全漏洞，影响范围包括数十种路由器型号。这个漏洞是 Trustwave 蜘蛛实验室的研究专家 Simon Kenin 发现的，因为 Netgear 路由器的密码恢复流程存在缺陷，入侵者可以利用这个漏洞绕过 Netgear 路由器密码，在取得路由器的完全控制权之后，入侵者就能对路由器进行配置、将其变成僵尸网络、更甚者可以上传全新固件。Netgear 已经公布了所有受感染型号路由器的更新固件，强烈建议用户尽快更新自己的设备。

参考链接：http://www.freebuf.com/news/126063.html

2. Brave 浏览器被曝安全漏洞

安全研究人员 Aaditya Purani 在 Hackerone 发现，攻击者可以利用浏览器漏洞伪造网页进行网址欺骗，一旦用户点击访问就可能泄漏个人信息，攻击者更可以在虚假页面上实施挂马和钓鱼等行为。事实上，无论用户通过 Android 还是 IOS 的 Brave 客户端去访问他构造好的网址，URL 都会跳转到 https://facebook.com（你可以看到甚至还有绿锁安全认证），但页面却还是 Purani 预先写好的内容。Brave 安全团队早已于发现一周内修复了这个问题，因此暂无负面影响。

参考链接：http://www.freebuf.com/news/125166.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