国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2018 年 1 月 22 日-2018 年 1 月 28 日 **2018 年第 4 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 241 个，其中高危漏洞 109 个、中危漏洞 115 个、低危漏洞 17 个。漏洞平均分值为 6.58。本周收录的漏洞中，涉及 0day 漏洞 30 个（占 12%），其中互联网上出现“Joomla! JEX TN Video Gallery extension SQL 注入漏洞、GetGo Download Manager 缓冲区溢出漏洞”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 671 个，与上周（532 个）环比增长 26%。

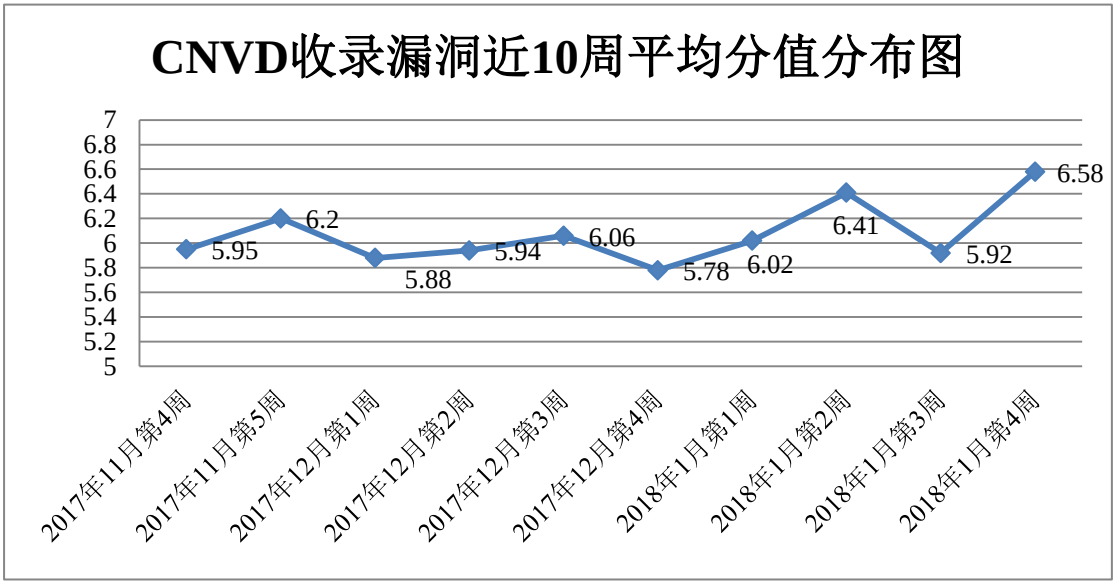

图 1 CNVD 收录漏洞近 10 周平均分值分布图

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，安天实验室、华为技术有限公司、恒安嘉新、天融信、H3C 等单位报送数量较多。四川虹微技术有限公司（子午攻防实验室）、南京联成科技发展股份有限公司、中新网络信息安全股份有限公司、上海观安信息技术股份有

限公司、北京同余科技有限公司、蚂蚁金服巴斯光年实验室、上海银基信息安全技术股份有限公司、福建省海峡信息技术有限公司及其他个人白帽子向 CNVD 提交了 671 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
网神	229	229
安天实验室	222	0
华为技术有限公司	173	0
恒安嘉新	166	0
天融信	107	1
H3C	93	0
漏洞盒子	78	78
北京数字观星科技有限公司	58	0
绿盟科技	53	0
杭州安恒信息技术有限公司	48	0
卫士通信息产业股份有限公司	43	0
中国电信集团系统集成有限责任公司	39	0
北京无声信息技术有限公司	33	0
知道创宇	3	3
四川虹微技术有限公司（子午攻防实验室）	93	93
南京联成科技发展股份有限公司	47	47
中新网络信息安全股份有限公司	6	6
上海观安信息技术股份有限公司	2	2
北京同余科技有限公司	1	1

蚂蚁金服巴斯光年实验室	1	1
上海银基信息安全技术股份有限公司	1	1
福建省海峡信息技术有限公司	1	1
CNCERT 重庆分中心	19	19
CNCERT 江西分中心	13	13
CNCERT 山西分中心	10	10
CNCERT 贵州分中心	7	7
CNCERT 福建分中心	5	5
CNCERT 陕西分中心	4	4
CNCERT 广东分中心	3	3
CNCERT 天津分中心	3	3
CNCERT 甘肃分中心	2	2
CNCERT 河北分中心	2	2
CNCERT 吉林分中心	2	2
CNCERT 浙江分中心	2	2
CNCERT 海南分中心	1	1
CNCERT 新疆分中心	1	1
个人	134	134
报送总计	1705	671

本周漏洞按类型和厂商统计

本周，CNVD 收录了 241 个漏洞。其中应用程序漏洞 155 个，WEB 应用漏洞 42 个，网络设备漏洞 32 个，数据库漏洞 6 个，安全产品漏洞 5 个，操作系统漏洞 1 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	155
WEB 应用漏洞	42
网络设备漏洞	32
数据库漏洞	6
安全产品漏洞	5
操作系统漏洞	1

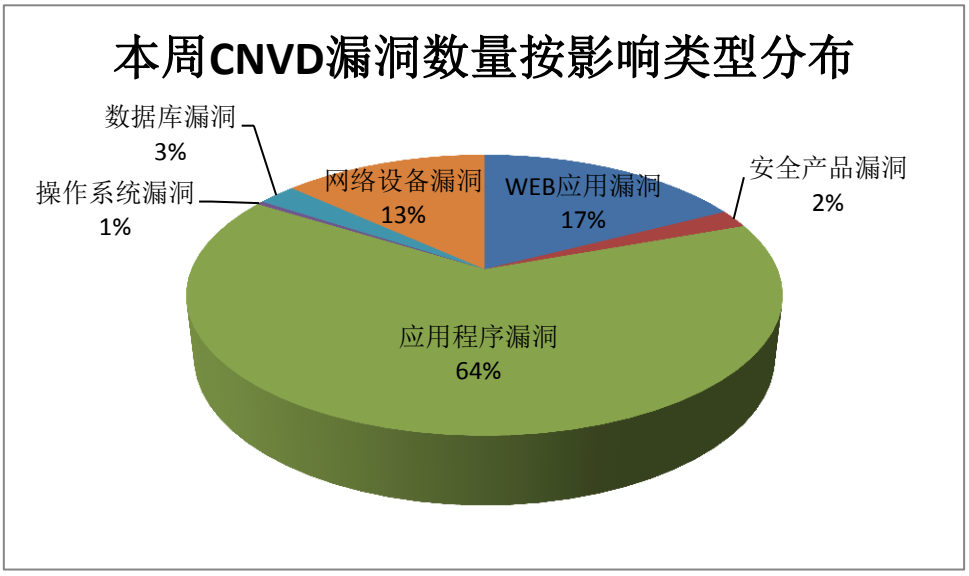

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Oracle、TP-Link、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。

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	Oracle	86	36%
2	TP-Link	24	10%
3	Cisco	15	6%
4	ImageMagick	6	2%
5	PHP Scripts Mall	5	2%
6	Dolibarr	4	2%
7	Kazuho Oku	4	2%
8	Joomla!	3	1%
9	Advantech	2	1%
10	其他	92	38%

本周行业漏洞收录情况

本周，CNVD 收录了 44 个电信行业漏洞，7 个移动互联网行业漏洞，4 个工控行业漏洞（如下图所示）。其中，“Cisco StarOS 命令注入漏洞、Oracle MySQL Server 存在未明漏洞（CNVD-2018-02063）、Siemens DESIGO PX 固件文件上传漏洞、Siemens S7-300 PLC 通讯模块存在命令执行漏洞、ALLPlayer ALLMediaServer MediaServer.exe 文件缓冲区溢出漏洞”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/

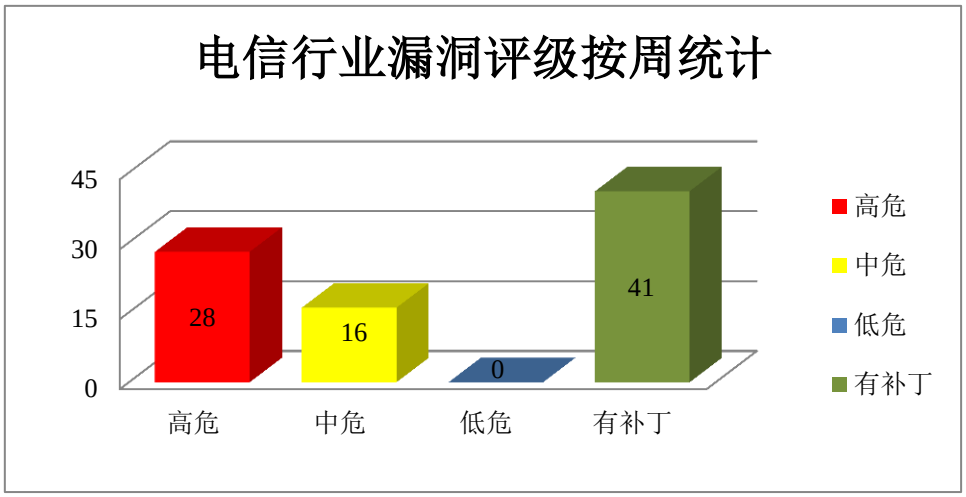

图 3 电信行业漏洞统计

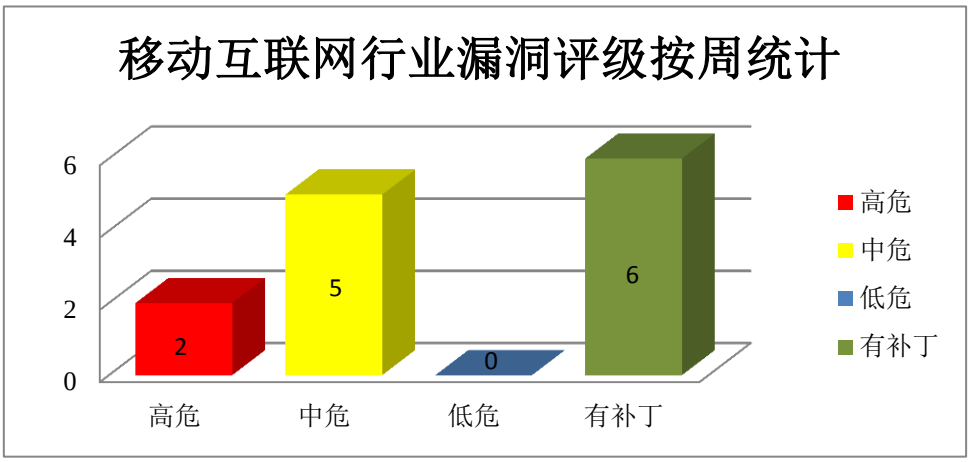

图 4 移动互联网行业漏洞统计

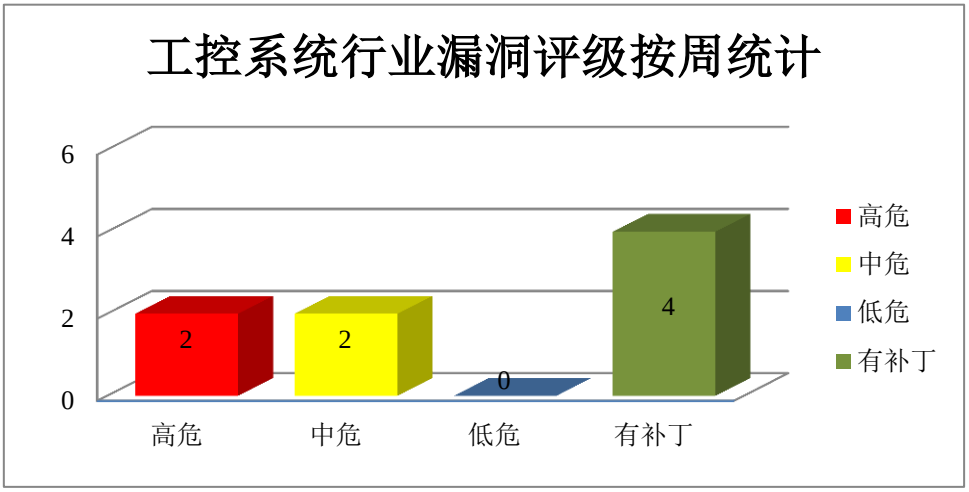

图 5 工控行业漏洞统计

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、OAuth 2.0 存在第三方帐号快捷登录授权劫持漏洞

OAuth（Open Authorization）是一个关于授权的开放网络标准。本周，该产品被披露存在第三方帐号快捷登录授权劫持漏洞，攻击者可通过登录受害者账号，获取存储在第三方移动应用上的敏感信息。

CNVD 收录的相关漏洞包括：OAuth 2.0 存在第三方帐号快捷登录授权劫持漏洞。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-2018-01622

2、Oracle 产品安全漏洞

Oracle Hyperion 是美国甲骨文（Oracle）公司的一套财务建模应用软件。Oracle Sun Systems Products Suite 是 Sun 系统产品包。Oracle VM VirtualBox 是其中的一个虚拟机组件。Oracle MySQL 是一套开源的关系数据库管理系统。本周，上述产品被披露存在未明和权限提升漏洞，攻击者可利用该漏洞控制组件，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 Hyperion Planning 组件存在未明漏洞、Oracle Sun Systems Products Suite 存在未明漏洞（CNVD-2018-01953、CNVD-2018-01954）、Oracle VM VirtualBox 权限提升漏洞（CNVD-2018-02055、CNVD-2018-02056、CNVD-2018-02061、CNVD-2018-02062）、Oracle MySQL Server 存在未明漏洞（CNVD-2018-02063）。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-2018-01529

http://www.cnvd.org.cn/flaw/show/CNVD-2018-01953

http://www.cnvd.org.cn/flaw/show/CNVD-2018-01954

http://www.cnvd.org.cn/flaw/show/CNVD-2018-02055

http://www.cnvd.org.cn/flaw/show/CNVD-2018-02056

http://www.cnvd.org.cn/flaw/show/CNVD-2018-02061

http://www.cnvd.org.cn/flaw/show/CNVD-2018-02062

http://www.cnvd.org.cn/flaw/show/CNVD-2018-02063

3、TP-Link 产品安全漏洞

TP-Link WVR、WAR 和 ER devices 都是中国普联（TP-LINK）公司的不同系列的路由器产品。本周，上述产品被披露存在任意命令执行漏洞，远程攻击者可通过文件中的变量注入命令利用该漏洞执行任意命令。

CNVD 收录的相关漏洞包括：TP-Link WVR、WAR 和 ER 设备任意命令执行漏洞（CNVD-2018-01907、CNVD-2018-01908、CNVD-2018-01909、CNVD-2018-01910、CNVD-2018-01911、CNVD-2018-01912、CNVD-2018-01913、CNVD-2018-01914）。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-2018-01907

http://www.cnvd.org.cn/flaw/show/CNVD-2018-01908

http://www.cnvd.org.cn/flaw/show/CNVD-2018-01909

http://www.cnvd.org.cn/flaw/show/CNVD-2018-01910

http://www.cnvd.org.cn/flaw/show/CNVD-2018-01911

http://www.cnvd.org.cn/flaw/show/CNVD-2018-01912

http://www.cnvd.org.cn/flaw/show/CNVD-2018-01913

http://www.cnvd.org.cn/flaw/show/CNVD-2018-01914

4、Cisco 产品安全漏洞

Cisco Prime Infrastructure 是美国思科（Cisco）公司的一套技术进行无线管理的解决方案。Cisco IOS Software/NX-OS System 是一套操作系统。Cisco StarOS operating system 是一套虚拟化操作系统。Cisco WebEx Meetings Server 是一套包含音频、视频和 Web 会议的多功能会议解决方案。Cisco Prime Service Catalog（PSC）是一套通过单一的门户网站提供所有 IT 服务的服务目录解决方案。Cisco Small Business Managed Switches software 是一套交换机管理软件。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞提升权限或发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Cisco Prime Infrastructure 权限提升漏洞（CNVD-2018-02043）、Cisco IOS Software 拒绝服务漏洞（CNVD-2018-02048）、Cisco StarOS 命令注入漏洞、Cisco WebEx Meetings Server 权限提升漏洞、Cisco Prime Service Catal

og 跨站请求伪造漏洞、Cisco Small Business Switches 跨站脚本漏洞、Cisco NX-OS System Software 未授权操作漏洞、Cisco Small Business 300 and 500 Series HTTP 响应拆分漏洞。其中“Cisco Prime Infrastructure 权限提升漏洞（CNVD-2018-02043）、Cisco IOS Software 拒绝服务漏洞（CNVD-2018-02048）、Cisco StarOS 命令注入漏洞”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-2018-02043
http://www.cnvd.org.cn/flaw/show/CNVD-2018-02048
http://www.cnvd.org.cn/flaw/show/CNVD-2018-02053
http://www.cnvd.org.cn/flaw/show/CNVD-2018-02054
http://www.cnvd.org.cn/flaw/show/CNVD-2018-02041
http://www.cnvd.org.cn/flaw/show/CNVD-2018-02050
http://www.cnvd.org.cn/flaw/show/CNVD-2018-02052
http://www.cnvd.org.cn/flaw/show/CNVD-2018-02049

5、 Joomla! JEXTN FAQ Pro extension SQL 注入漏洞

Joomla!是美国 Open Source Matters 团队开发的一套开源的内容管理系统(CMS)，本周，Joomla!被披露存在 SQL 注入漏洞，攻击者可借助 view=category 操作中的‘id’参数利用该漏洞注入 SQL 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-2018-01623

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

表 4 部分重要高危漏洞列表

CNVD 编号	漏洞名称	综合评级	修复方式
CNVD-2018-01631	Auth0 passport-wsfed-saml2 权限提升漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://auth0.com/docs/security/bulletins/cve-2017-16897
CNVD-2018-01940	Mozilla Thunderbird 命令执行漏洞	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://www.mozilla.org/en-US/security/advisories/mfsa2017-30/
CNVD-2018-02025	Siemens S7-300 PLC 通讯模块存在命令执行漏洞	高	厂商已提供漏洞修补方案，请关注厂商主页及时更新：https://www.siemens.com/cn/zh/home.html
CNVD-201	Siemens DESIGO PX 固件文	高	目前厂商已经发布了升级补丁以修复

8-01794	件上传漏洞		此安全问题，详情请关注厂商主页：https://www.siemens.com/cert/advisories
CNVD-2018-01931	Polycom HDX 端点远程执行代码漏洞	高	用户可联系供应商获得补丁信息：http://www.polycom.com/
CNVD-2018-01941	puppetlabs-mysql 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://puppet.com/security/cve/CVE-2015-7224
CNVD-2018-01641	Dolibarr ERP/CRM SQL 注入漏洞（CNVD-2018-01641）	高	厂商已发布漏洞修复程序，请及时关注更新：https://github.com/Dolibarr/dolibarr/commit/4a5988accbb770b74105baacd5a034689272128c
CNVD-2018-01643	Dolibarr ERP/CRM SQL 注入漏洞（CNVD-2018-01643）	高	厂商已发布漏洞修复程序，请及时关注更新：https://github.com/Dolibarr/dolibarr/commit/4a5988accbb770b74105baacd5a034689272128c
CNVD-2018-01644	Dolibarr ERP/CRM SQL 注入漏洞（CNVD-2018-01644）	高	厂商已发布漏洞修复程序，请及时关注更新：https://github.com/Dolibarr/dolibarr/commit/4a5988accbb770b74105baacd5a034689272128c
CNVD-2018-01943	Sony Music Center for PC 不可信搜索路径漏洞	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://musiccenter.sony.net

小结：本周，OAuth 2.0 存在第三方帐号快捷登录授权劫持漏洞，攻击者可通过登录受害者账号，获取存储在第三方移动应用上的敏感信息。此外，Oracle、TP-Link、Cisco 等多款产品被披露存在多个漏洞，攻击者可利用漏洞提升权限、任意命令执行或造发起拒绝服务攻击等。另外，Joomla! JEXTN FAQ Pro extension SQL 注入漏洞，攻击者可借助 view=category 操作中的‘id’参数利用该漏洞注入 SQL 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. 通过 adbd 配置漏洞在安卓设备上提升权限

近日，Android 上的一个本地提权漏洞已被确认，该漏洞可通过设备上运行的 Android Debug Bridge Daemon（adbd）被利用。

如果一个安卓设备被发现正在运行于 TCP 端口监听的 adbd，那么设备上运行的恶意程序就可以进行连接和身份验证，从而实现提权。该漏洞影响版本为 Android 4.2.2

到 Android 8.0，编号为 CVE-2017-13212。利用这种错误配置可以允许安卓应用从“u:r:untrusted_app:s0”提升为“u:r:shell:s0”

参考链接：http://www.freebuf.com/vuls/161150.html

2. Hadoop 大数据平台 YARN NodeManager 漏洞 CVE-2017-15718

近日，Apache Hadoop 大数据平台的 YARN NodeManager 爆出信息泄露漏洞，CVE 编号 CVE-2017-15718，攻击者可能获得应用密码。受影响版本 Apache Hadoop 2.7.3 及 2.7.4，之前为 cve-2016-3086 提供的安全性修复是不完整的。

YARN NodeManager 泄漏凭证存储提供程序的密码，该凭据由 nodemanager 用于 YARN 应用。如果你使用 credentialprovider 功能加密密码并应用于 nodemanager 配置，nodemanager 启动的任何容器都有可能获取加密密码。其他密码本身不直接暴露。

参考链接：http://toutiao.secjia.com/cve-2017-15718

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