国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2018 年 2 月 5 日-2018 年 2 月 11 日 **2018 年第 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 284 个，其中高危漏洞 114 个、中危漏洞 144 个、低危漏洞 26 个。漏洞平均分值为 6.13。本周收录的漏洞中，涉及 0day 漏洞 102 个（占 36%），其中互联网上出现“Joomla! JMS Music SQL 注入漏洞、RAVPower Filehub 远程代码执行漏洞”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 495 个，与上周（581）个环比降低 15%。

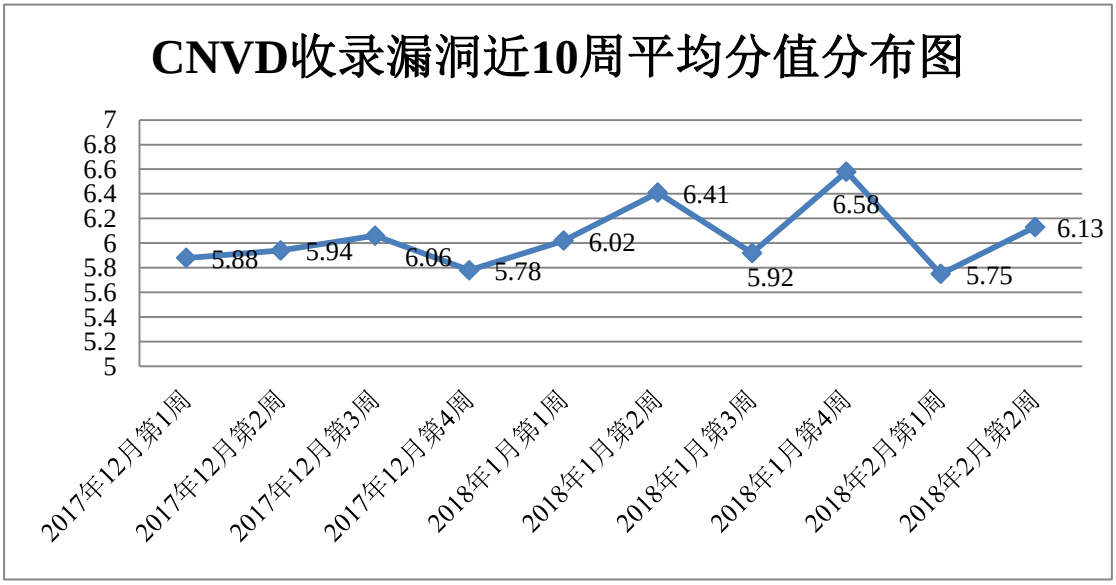

图 1 CNVD 收录漏洞近 10 周平均分值分布图

本周漏洞事件处置情况

本周，CNVD 向基础电信企业通报漏洞事件 2 起，向银行、证券、保险、能源等重要行业单位通报漏洞事件 25 起，协调 CNCERT 各分中心验证和处置涉及地方重要部门漏洞事件 235 起，协调教育行业应急组织验证和处置高校科研院所系统漏洞事件 73 起，

向国家上级信息安全协调机构上报涉及部委门户、子站或直属单位信息系统漏洞事件 23 起。

此外，CNVD 通过已建立的联系机制或涉事单位公开联系渠道向以下单位通报了其信息系统或软硬件产品存在的漏洞，具体处置单位情况如下所示：

金山软件股份有限公司、郑州商帮网络科技有限公司、中国储备粮管理总公司、用友网络科技股份有限公司、INFRAWARE 公司、酷溜网（北京）科技有限公司、广州网天网络科技有限公司、成都天睿信息技术有限公司、深圳市集时通讯股份有限公司、北京江民新科技术有限公司、北京棣南新宇科技有限公司、北京安证通信息科技股份有限公司、上海亿速网络科技有限公司、江西金磊科技发展有限公司、中控太科（上海）电子科技有限公司、南昌腾速科技有限公司、上海求创科技有限公司、灵宝简好网络科技有限公司、武汉达梦数据库有限公司、北京海腾时代科技有限公司、深圳市锟铻科技有限公司、郑州江山科技有限公司、常州百图群星文化传媒有限公司、北京盛拓鸿远信息技术有限公司、中控太科（上海）电子科技有限公司、北京百卓网络技术有限公司、谷歌公司、phpmywind、Duomicms、DWG TOOL Software、Shop7z、天睿程序设计团队、老 y 文章管理系统、国家摩托车质量监督检验中心、睿思设计、无忧网络、嘉義縣 CMS 管理資訊系統、新能源汽车国家监测与管理中心、ykcms、大米 CMS、校无忧科技。

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，天融信、华为技术有限公司、哈尔滨安天科技股份有限公司、新华三技术有限公司、北京神州绿盟科技有限公司等单位报送公开收集的漏洞数量较多。四川虹微技术有限公司（子午攻防实验室）、福建省海峡信息技术有限公司、北京安华金和科技有限公司、中新网络信息安全股份有限公司、北京长亭科技有限公司、南瑞集团公司（国网电力科学研究院）、广州万方计算机科技有限公司、杭州安信检测技术有限公司及其他个人白帽子向 CNVD 提交了 495 个以事件型漏洞为主的原创漏洞，其中包括 360 网神（补天平台）和漏洞盒子向 CNVD 共享的白帽子报送的 223 条原创漏洞信息。

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
天融信	208	4
华为技术有限公司	186	0
哈尔滨安天科技股份有限公司	174	0
新华三技术有限公司	162	0

360 网神(补天平台)	154	154
北京神州绿盟科技有限公司	127	0
恒安嘉新(北京)科技股份公司	80	0
漏洞盒子	69	69
杭州安恒信息技术有限公司	40	0
北京数字观星科技有限公司	30	0
中国电信集团系统集成有限责任公司	29	0
卫士通信息产业股份有限公司	23	0
北京无声信息技术有限公司	11	0
知道创宇	2	0
四川虹微技术有限公司（子午攻防实验室）	69	69
福建省海峡信息技术有限公司	12	12
北京安华金和科技有限公司	9	9
中新网络信息安全股份有限公司	8	8
北京长亭科技有限公司	5	5
南瑞集团公司（国网电力科学研究院）	5	5
广州万方计算机科技有限公司	1	1
杭州安信检测技术有限公司	1	1
CNCERT 吉林分中心	8	8
CNCERT 新疆分中心	3	3
CNCERT 广东分中心	3	3
CNCERT 河北分中心	2	2

个人	142	142
报送总计	1563	495

本周漏洞按类型和厂商统计

本周，CNVD 收录了 284 个漏洞。其中应用程序漏洞 147 个，WEB 应用漏洞 82 个，安全产品漏洞 23 个，操作系统漏洞，19 个，网络设备漏洞 13 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	147
WEB 应用漏洞	82
安全产品漏洞	23
操作系统漏洞	19
网络设备漏洞	13

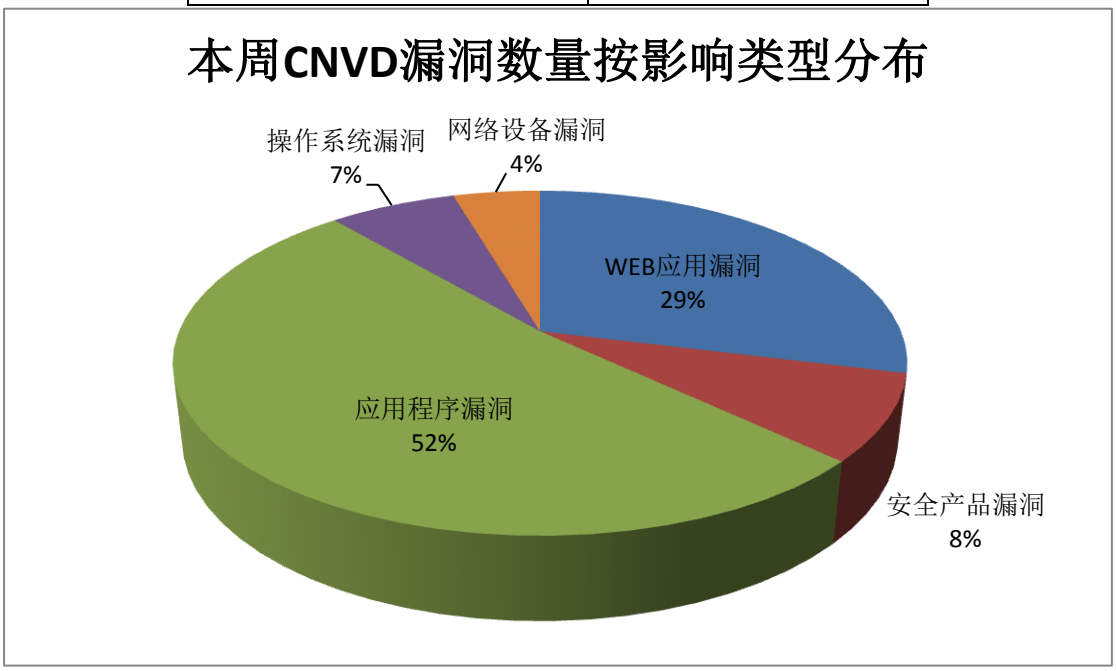

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Joomla!、X.org、Ethereum 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	Joomla!	12	4%
2	X.org	12	4%
3	Ethereum	10	4%

4	CloudBees	9	3%
5	Google	8	3%
6	Micropoint	7	2%
7	Support.com	6	2%
8	VMware	6	2%
9	Discuz!	5	2%
10	其他	209	74%

本周行业漏洞收录情况

本周，CNVD 收录了 11 个电信行业漏洞，15 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，“Fuji Electric V-Server VPR 堆栈缓冲区溢出漏洞、3S CODESYS WebVisu Web 服务器组件堆栈缓冲区溢出漏洞、Asus asuswrt 缓冲区溢出漏洞、IBM WebSphere Application Server 权限提升漏洞、Google Android LG Bootloader 组件权限提升漏洞”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/

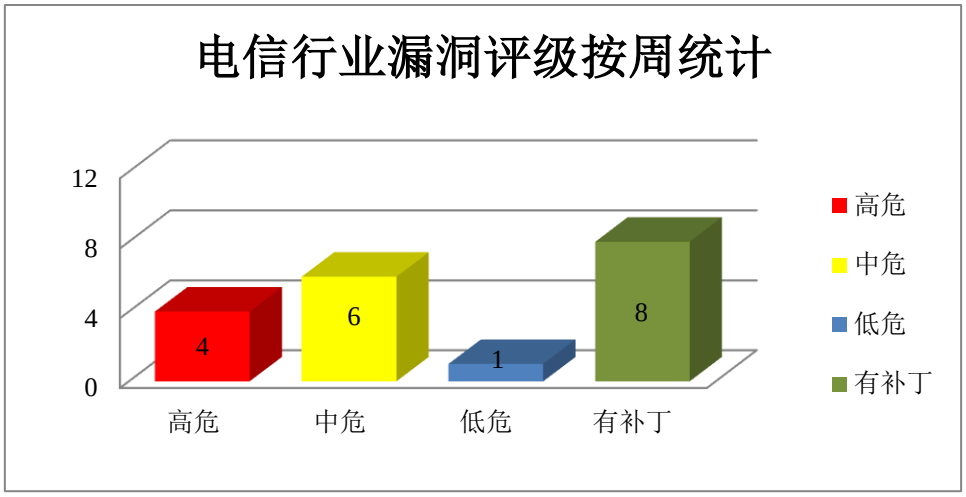

图 3 电信行业漏洞统计

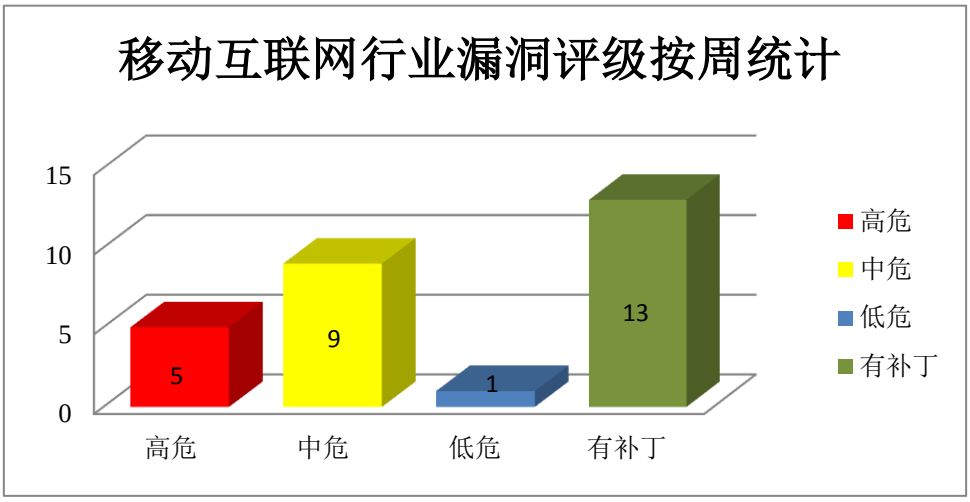

图 4 移动互联网行业漏洞统计

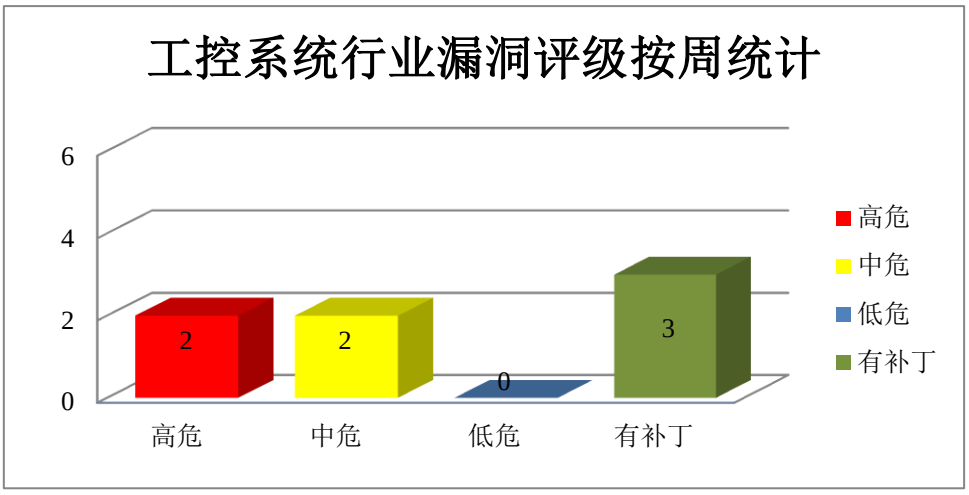

图 5 工控行业漏洞统计

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、Google 产品安全漏洞

Google Chrome OS 是美国谷歌（Google）公司开发的一套开源操作系统。Google Go 是一种针对多处理器系统应用程序的编程进行了优化的编程语言。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、执行任意命令或绕过安全限制等。

CNVD 收录的相关漏洞包括：Google Android LG Bootloader 组件权限提升漏洞、Google Android MTK Media 权限提升漏洞、Google Chrome for Mac、Windows 和 Linux libxml2 整数溢出漏洞、Google Go 命令执行漏洞、Google Android Media framework 权限提升漏洞（CNVD-2018-03093）、Google Android NVIDIA 组件权限提升漏洞（CNVD-2018-02982）、Google Android SensorService 存在空指针引用漏洞、Google Chrome OS ChromeVox 中间人安全绕过漏洞。其中，“Google Android LG Bootloader 组件

权限提升漏洞、Google Android MTK Media 权限提升漏洞、Google Chrome for Mac、Windows 和 Linux libxml2 整数溢出漏洞、Google Go 命令执行漏洞”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-2018-03092
http://www.cnvd.org.cn/flaw/show/CNVD-2018-03094
http://www.cnvd.org.cn/flaw/show/CNVD-2018-03177
http://www.cnvd.org.cn/flaw/show/CNVD-2018-03181
http://www.cnvd.org.cn/flaw/show/CNVD-2018-03093
http://www.cnvd.org.cn/flaw/show/CNVD-2018-02982
http://www.cnvd.org.cn/flaw/show/CNVD-2018-02911
http://www.cnvd.org.cn/flaw/show/CNVD-2018-03084

2、Joomla!产品安全漏洞

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，该产品被披露存在多个漏洞，攻击者可利用漏洞获取敏感信息、注入 SQL 命令或下载任意文件等。

CNVD 收录的相关漏洞包括：Joomla! Tumder SQL 注入漏洞、Joomla! LiveCRM SaaS Cloud SQL 注入漏洞、Joomla! JS Support Ticket 跨站请求伪造漏洞、Joomla! JMS Music SQL 注入漏洞、Joomla! jLike 组件信息泄露漏洞、Joomla! JSP Tickets SQL 注入漏洞、Joomla! Zh YandexMap SQL 注入漏洞、Joomla! Zh GoogleMap SQL 注入漏洞。除“Joomla! JS Support Ticket 跨站请求伪造漏洞、Joomla! jLike 组件信息泄露漏洞”外，其余漏洞的综合评级为“高危”。目前，厂商尚未发布上述漏洞的修补程序。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-2018-02805
http://www.cnvd.org.cn/flaw/show/CNVD-2018-02806
http://www.cnvd.org.cn/flaw/show/CNVD-2018-02809
http://www.cnvd.org.cn/flaw/show/CNVD-2018-02807
http://www.cnvd.org.cn/flaw/show/CNVD-2018-02955
http://www.cnvd.org.cn/flaw/show/CNVD-2018-02974
http://www.cnvd.org.cn/flaw/show/CNVD-2018-02983
http://www.cnvd.org.cn/flaw/show/CNVD-2018-02993

3、X.org 产品安全漏洞

xorg-x11-server 是多个厂商操作系统中所捆绑的 X 窗口系统显示服务器。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或执行任意代码。

CNVD 收录的相关漏洞包括：xorg-x11-server 拒绝服务漏洞（CNVD-2018-03105、

CNVD-2018-03146、CNVD-2018-03148、CNVD-2018-03149、CNVD-2018-03150、CNVD-2018-03151、CNVD-2018-03152、CNVD-2018-03153）。上述综合评级为“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-2018-03105

http://www.cnvd.org.cn/flaw/show/CNVD-2018-03146

http://www.cnvd.org.cn/flaw/show/CNVD-2018-03148

http://www.cnvd.org.cn/flaw/show/CNVD-2018-03149

http://www.cnvd.org.cn/flaw/show/CNVD-2018-03150

http://www.cnvd.org.cn/flaw/show/CNVD-2018-03151

http://www.cnvd.org.cn/flaw/show/CNVD-2018-03152

http://www.cnvd.org.cn/flaw/show/CNVD-2018-03153

4、Micropoint 产品安全漏洞

Micropoint proactive defense software 是中国东方微点（Micropoint）公司的一套第三代反病毒软件。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：Micropoint Proactive Defense Software拒绝服务漏洞、Micropoint Proactive Defense Software 拒绝服务漏洞（CNVD-2018-02956、CNVD-2018-02957、CNVD-2018-02958、CNVD-2018-02975、CNVD-2018-02977、CNVD-2018-02978）。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-2018-02976

http://www.cnvd.org.cn/flaw/show/CNVD-2018-02956

http://www.cnvd.org.cn/flaw/show/CNVD-2018-02957

http://www.cnvd.org.cn/flaw/show/CNVD-2018-02958

http://www.cnvd.org.cn/flaw/show/CNVD-2018-02975

http://www.cnvd.org.cn/flaw/show/CNVD-2018-02977

http://www.cnvd.org.cn/flaw/show/CNVD-2018-02978

5、 Adobe Flash Player 内存错误引用远程代码执行漏洞（CNVD-2018-02962）

Adobe Flash Player 是一种广泛使用的、专有的多媒体程序播放器。本周，Adobe 被披露存在内存错误引用远程代码执行漏洞，攻击者可利用漏洞触发释放后重用内存错误并在目标用户的系统上执行任意代码。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-2018-02962

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-2018-02834	CloudBees Jenkins EC2 Plugin 任意命令执行漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://jenkins.io/security/advisory/2017-12-06/
CNVD-2018-02835	CloudBees Jenkins 竞争条件漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://jenkins.io/security/advisory/2017-12-14/
CNVD-2018-02920	Asus asuswrt 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://sploit.tech/2018/01/16/ASUS-part-I.html
CNVD-2018-02919	Asus asuswrt 会话令牌可预测漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：http://seclists.org/fulldisclosure/2018/Jan/63
CNVD-2018-03038	VMware vSphere Data Protection 任意文件上传漏洞	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.emc.com/
CNVD-2018-03039	VMware vSphere Data Protection 目录遍历漏洞	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.emc.com/
CNVD-2018-03060	QEMU 拒绝服务漏洞（CNVD-2018-03060）	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.qemu.org/
CNVD-2018-03113	Xplico 任意命令执行漏洞	高	目前厂商已发布漏洞修复程序，请及时关注更新：https://www.xplico.org/archives/1538
CNVD-2018-03166	Irssi 缓冲区溢出漏洞	高	目前厂商已发布漏洞修复程序，请及时关注更新：https://irssi.org/security/irssi_sa_2018_01.txt
CNVD-2018-03170	Irssi 空指针解引用漏洞（CNVD-2018-03170）	高	目前厂商已发布漏洞修复程序，请及时关注更新：https://irssi.org/security/irssi_sa_2018_01.txt

小结：本周，Google 被披露存在多个漏洞，攻击者可利用漏洞提升权限、执行任意命令或绕过安全限制等。此外，Joomla!、X.org、Micropoint 等多款产品被披露存在多个漏洞，攻击者可利用漏洞执行任意代码、发起拒绝服务攻击或提升权限等。另外，A

dobe 被披露存在内存错误引用远程代码执行漏洞，攻击者可利用漏洞触发释放后重用内存错误并在目标用户的系统上执行任意代码。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。

本周重要漏洞攻击验证情况

本周，CNVD 建议注意防范以下已公开漏洞攻击验证情况。

1、RAVPower Filehub 远程代码执行漏洞

验证描述

RAVPower FileHub 是美国 RAVPower 公司的一款多功能数码设备。该设备同时具有读卡器、USB 存储以及 NAS 文件服务器等功能。HTTP Server 是其中的一个 HTTP 服务器。

RAVPower Filehub 存在远程代码执行漏洞。远程攻击者可利用该漏洞以 root 权限向文件系统上传文件并以同样的权限执行代码。

验证信息

POC 链接：https://www.exploit-db.com/exploits/43871/

参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2018-02999

信息提供者

华为技术有限公司

注：以上验证信息(方法)可能带有攻击性，仅供安全研究之用。请广大用户加强对漏洞的防范工作，尽快下载相关补丁。

本周漏洞要闻速递

1. 苹果 iOS iBoot 源码泄露

近日，开源代码分享网站 GitHub（软件项目托管平台）上有人共享了 iPhone 操作系统的核心组件源码，泄露的代码属于 iOS 安全系统的重要组成部分—— iBoot，iBoot 相当于是 Windows 电脑的 BIOS 系统。此次 iBoot 源码泄露可能让数以亿计的 iOS 设备面临安全威胁。iOS 与 MacOS 系统开发者 Jonathan Levin 表示，这是 iOS 历史上最严重的一次泄漏事件。苹果于当地时间 2018 年 2 月 8 日上午发表声明称，证实泄露到 GitHub 上的代码确实是 iBoot 源代码，但强调对 iPhone 安全没有影响。苹果方面认为，苹果产品的安全性并不取决于源代码的保密性。苹果的产品还内置了许多硬件和软件保护层来保障用户的安全。

参考链接：https://www.easyaq.com/news/618886048.shtml

2. 银联红包活动曝重大漏洞，可直接查看用户手机号

银联云闪付在春节期间推出了红包活动，但有网友在 V2EX 上反映，称该活动的分享页链接有重大漏洞，用户手机号有遭到泄露的风险。 按照官方的活动规则，用户在首次登陆云闪付 App 后，点击首页“红包到 福才到”进入活动页面，点击“开”就能领取 1 次随机红包，最高 2018 元！ 同时，该活动也支持分享，其他未下载的用户可以通过该链接下载云闪付后参与活动，但是银联将 Base64 的编码直接暴露在分享链接中。通过该编码可在 base64 的解码程序中直接查到用户手机账号。

参考链接：https://www.easyaq.com/news/445755677.shtml

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