国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2019 年 04 月 22 日-2019 年 04 月 28 日 **2019 年第 17 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 288 个，其中高危漏洞 104 个、中危漏洞 153 个、低危漏洞 31 个。漏洞平均分值为 5.85。本周收录的漏洞中，涉及 0day 漏洞 106 个（占 37%），其中互联网上出现“Laravel SQL 注入漏洞、NagiosXI 提权漏洞”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 2245 与上周（1994 个）环比增长 13%。

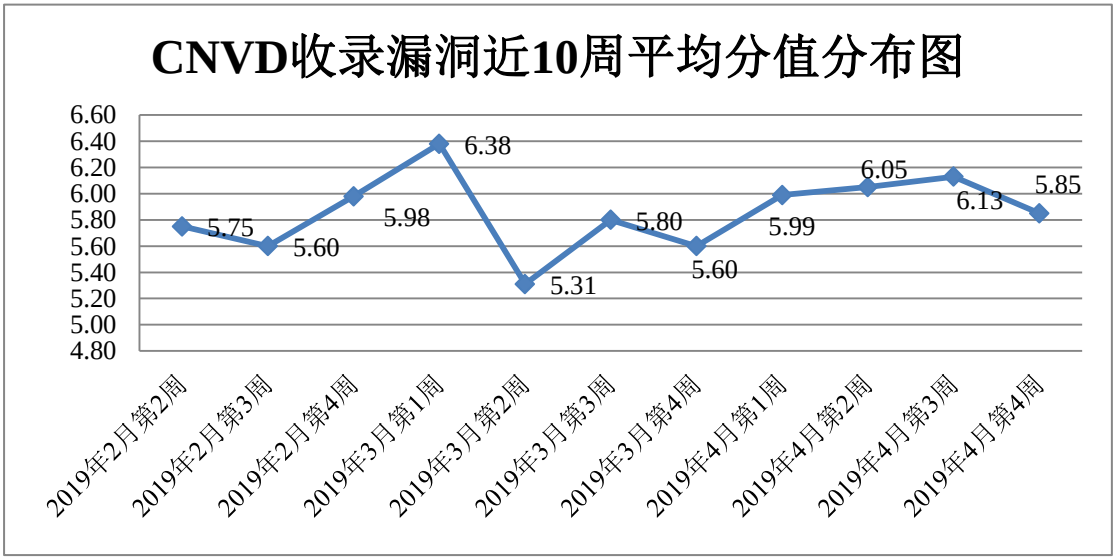

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 10 起，向银行、保险、能源等重要行业单位通报漏洞事件 50 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 515 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 44 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：沧州市凡诺广告传媒有限公司、成都我来啦网格信息技术有限公司、灵宝简好网络科技有限公司、北京小米科技有限责任公司、西安众邦网络科技有限公司、宁波慕枫网络科技有限公司、金山软件股份有限公司、合一信息技术（北京）有限公司、民生财富投资管理有限公司、无锡信捷电气股份有限公司、北京中网速通科技有限公司、环球车享汽车租赁有限公司、上海创旗天下科技股份有限公司、深圳市锟铻科技有限公司、佛山云迈电子商务有限公司、上海七慧网络科技有限公司、河北商之翼互联网科技有限公司、北京因酷时代科技有限公司、南大傲拓科技江苏股份有限公司、深圳市汇川技术股份有限公司、黄石市科威自控有限公司、昆明鼎华信息科技有限公司、深圳市合信自动化技术有限公司、中铁十一局集团城市轨道工程有限公司、北京慧萌信安软件技术有限公司、上海丹帆网络科技有限公司、武汉类森科技有限公司、汕头市金南曦文化传播有限公司、中铁十二局集团电气化工程有限公司、中铁五局集团有限公司、中航（宁夏）生物股份有限公司、北京世纪长秋科技有限公司、淮南市银泰软件科技有限公司、深圳市显控科技股份有限公司、福州富昌维控电子科技有限公司、太原迅易科技有限公司、北京外企人力资源服务有限公司、上海步科自动化股份有限公司、北京图灵开物技术有限公司、上海美橙科技信息发展有限公司、南京新迪生软件技术有限公司、云南航天工程物探检测股份有限公司、郑州微厦计算机科技有限公司、中铁物流集团、台达集团、中国管理科学研究院行业发展研究所、中铁二院工程集团有限责任公司测绘分院、中国通信工业协会、中国民族图书馆、食品机械设备网、中国招生信息网、中国研招网、财经调研网、21 地产网、特种劳动防护用品安全标志管理中心、动科企业网站管理系统、超级 cms、海洋 CMS、LS 产电、InduSoft、XnView、Zzzcms 和 JYmusic。

本周，CNVD 发布了《关于 Oracle WebLogic wls9-async 组件存在反序列化远程命令执行漏洞的安全公告（第二版）》。详情参见 CNVD 网站公告内容。

http://www.cnvd.org.cn/webinfo/show/4999

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，北京天融信网络安全技术有限公司、哈尔滨安天科技集团股份有限公司、新华三技术有限公司、华为技术有限公司、深信服科技股份有限公司等单位报送公开收集的漏洞数量较多。长春嘉诚信息技术股份有限公司、中新网络信息安全股份有限公司、上海并擎软件科技有限公司、国瑞数码零点实验室、任子行网络技术股份有限公司、安徽锋刃信息科技有限公司、山东云天安全技术有限公司、北京圣博润高新技术股份有限公司、南京联成科技发展股份有限公司、上海银基信息安全技术股份有限公司、重庆贝特计算机系统工程有限公司、山东华鲁科技发展股份有限公

司、山石网科通信技术股份有限公司、内蒙古奥创科技有限公司、四川虹微技术有限公司（子午攻防实验室）、中国交通通信信息中心、河南信安世纪科技有限公司、华信咨询设计研究院有限公司、江苏安又恒信息科技有限公司、江苏通付盾信息安全技术有限公司、上海观安信息技术股份有限公司、新疆海狼科技有限公司及其他个人白帽子向 CNVD 提交了 2245 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）和斗象科技（漏洞盒子）向 CNVD 共享的白帽子报送的 1494 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
斗象科技（漏洞盒子）	1031	1031
360 网神（补天平台）	463	463
北京天融信网络安全技术有限公司	329	6
哈尔滨安天科技集团股份有限公司	299	0
新华三技术有限公司	236	0
华为技术有限公司	101	0
深信服科技股份有限公司	81	0
北京启明星辰信息安全技术有限公司	51	8
北京神州绿盟科技有限公司	46	31
恒安嘉新(北京)科技股份公司	34	0
北京数字观星科技有限公司	32	0
中国电信集团系统集成有限责任公司	15	0
厦门服云信息科技有限公司	5	0
四川无声信息技术有限公司	2	2
北京知道创宇信息技术有限公司	1	0
长春嘉诚信息技术股份有限公司	109	109
中新网络信息安全股份有限公司	84	84

上海并擎软件科技有限公司	73	73
国瑞数码零点实验室	66	66
任子行网络技术股份有限公司	51	51
安徽锋刃信息科技有限公司	40	40
山东云天安全技术有限公司	23	23
北京圣博润高新技术股份有限公司	17	17
南京联成科技发展股份有限公司	13	13
上海银基信息安全技术股份有限公司	13	13
重庆贝特计算机系统工程有限公司	12	12
山东华鲁科技发展股份有限公司	10	10
山石网科通信技术股份有限公司	2	2
内蒙古奥创科技有限公司	2	2
四川虹微技术有限公司（子午攻防实验室）	2	2
中国交通通信信息中心	1	1
河南信安世纪科技有限公司	1	1
华信咨询设计研究院有限公司	1	1
江苏安又恒信息科技有限公司	1	1
江苏通付盾信息安全技术有限公司	1	1
上海观安信息技术股份有限公司	1	1
新疆海狼科技有限公司	1	1
CNCERT 天津分中心	12	12
CNCERT 河北分中心	8	8

CNCERT 甘肃分中心	7	7
CNCERT 贵州分中心	3	3
CNCERT 四川分中心	1	1
CNCERT 浙江分中心	1	1
个人	148	148
报送总计	3430	2245

本周漏洞按类型和厂商统计

本周，CNVD 收录了 288 个漏洞。应用程序 157 个，WEB 应用 81 个，操作系统 23 个，数据库 21 个，智能设备（物联网终端设备）漏洞 5 个，网络设备（交换机、路由器等网络端设备）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	157
WEB 应用	81
操作系统	23
数据库	21
智能设备（物联网终端设备）漏洞	5
网络设备（交换机、路由器等网络端设备）	1

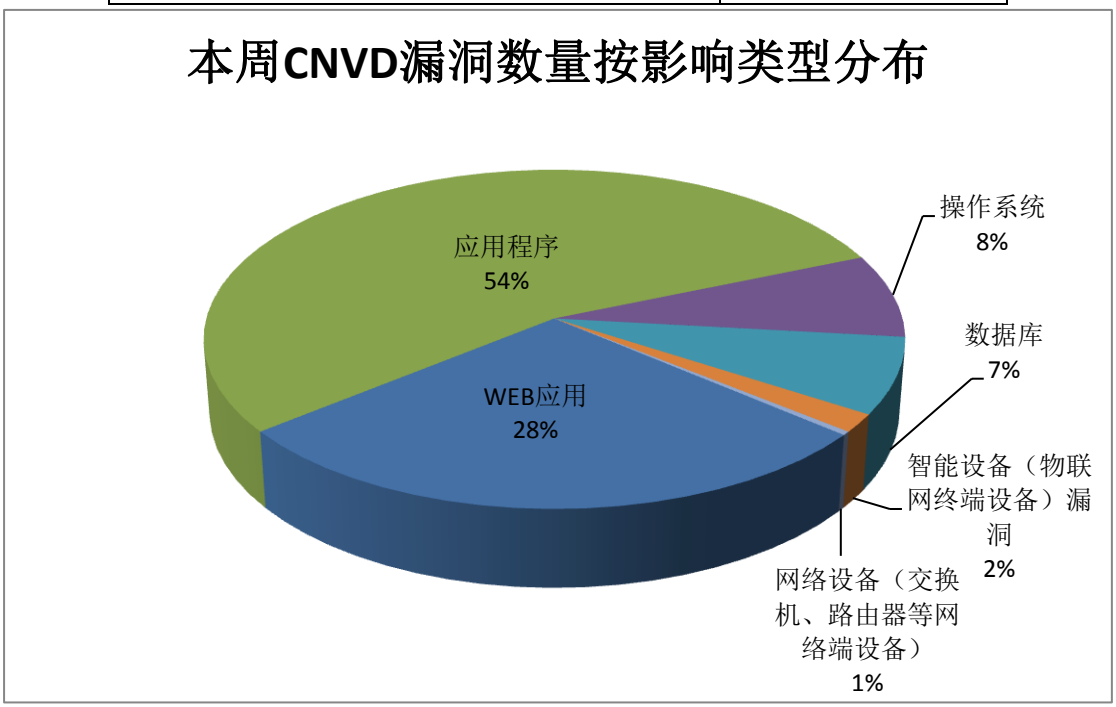

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Apple、Oracle、Adobe 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	Apple	22	8%
2	Oracle	22	8%
3	Adobe	20	7%
4	Cybozu	20	7%
5	Jfinal cms	12	4%
6	Wireshark	11	4%
7	GNU	10	3%
8	Xnview	10	3%
9	iDreamSoft	8	3%
10	其他	153	53%

本周行业漏洞收录情况

本周，CNVD 收录了 11 个电信行业漏洞，14 个移动互联网行业漏洞（如下图所示）。其中，“Oracle MySQL Server 拒绝服务漏洞（CNVD-2019-11750、CNVD-2019-11751、CNVD-2019-11752、CNVD-2019-11753、CNVD-2019-11754）”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/

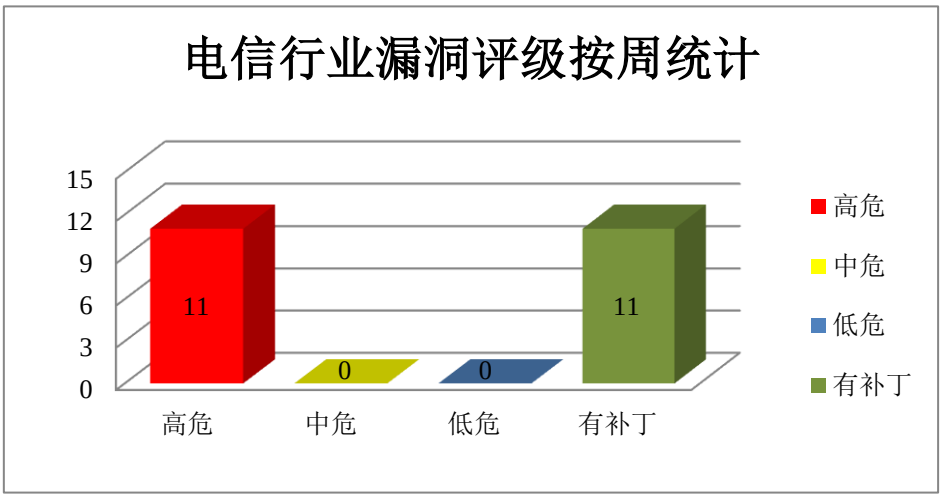

图 3 电信行业漏洞统计

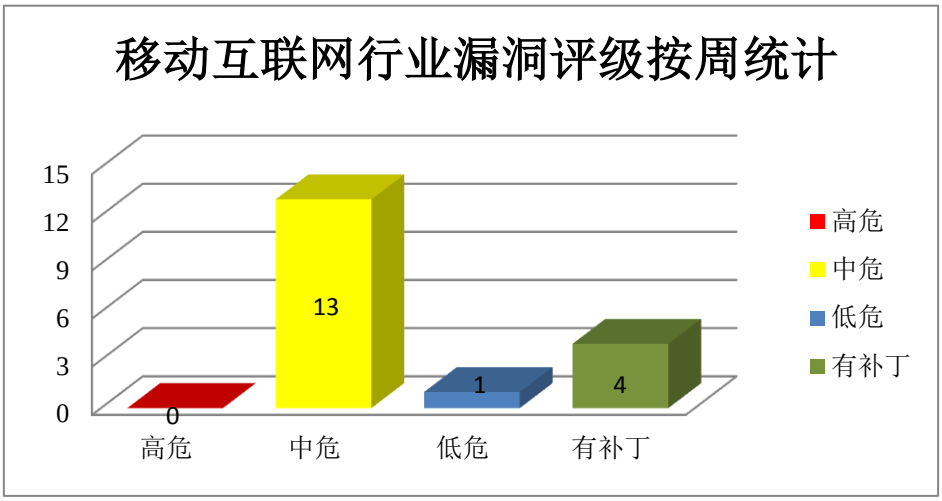

图 4 移动互联网行业漏洞统计

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、Apple 产品安全漏洞

Apple Xcode 是一套向开发人员提供的集成开发环境，它主要用于开发 Mac OS X 和 iOS 的应用程序。LLVM（Low Level Virtual Machine）是 LLVM 团队开发的一套构架编译器（compiler）的框架系统。Apple iOS 是为移动设备所开发的一套操作系统。tvOS 是一套智能电视操作系统。Safari 是开发的一款 Web 浏览器，是 MacOSX 和 iOS 操作系统附带的默认浏览器。WebKit 是其中的一个 Web 浏览器引擎组件。Apple macOS Sierra 是为 Mac 计算机所开发的一套专用操作系统。Apple OS X El Capitan 是一套专为 Mac 计算机所开发的专用操作系统。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信息，以内核权限执行任意代码。

CNVD 收录的相关漏洞包括：Apple Xcode LLVM 组件内存破坏漏洞、多款 Apple 产品 WebKit 组件内存破坏漏洞（CNVD-2019-12484）、Apple macOS High Sierra、OS X El Capitan 和 macOS Sierra SIP 组件配置错误漏洞、Apple macOS High Sierra AMD 组件信息泄露漏洞、多款 Apple 产品 Heimdal 组件内存破坏漏洞（CNVD-2019-12496、CNVD-2019-12497）、Apple iOS Core Bluetooth 组件内存破坏漏洞、Apple macOS High Sierra 和 Apple macOS Mojave Intel Graphics Driver 组件内存破坏漏洞。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-2019-12482

http://www.cnvd.org.cn/flaw/show/CNVD-2019-12484

http://www.cnvd.org.cn/flaw/show/CNVD-2019-12485

http://www.cnvd.org.cn/flaw/show/CNVD-2019-12486

http://www.cnvd.org.cn/flaw/show/CNVD-2019-12496

http://www.cnvd.org.cn/flaw/show/CNVD-2019-12497

http://www.cnvd.org.cn/flaw/show/CNVD-2019-12498

http://www.cnvd.org.cn/flaw/show/CNVD-2019-12502

2、Oracle 产品安全漏洞

Oracle MySQL 是一套开源的关系数据库管理系统。MySQL Server 是其中的一个数据库服务器组件。本周，上述产品被披露存在多个拒绝服务漏洞，攻击者可利用漏洞造成拒绝服务（挂起或频繁崩溃），影响数据的可用性。

CNVD 收录的相关漏洞包括：Oracle MySQL Server 拒绝服务漏洞（CNVD-2019-11751、CNVD-2019-11750、CNVD-2019-11753、CNVD-2019-11752、CNVD-2019-11755、CNVD-2019-11754、CNVD-2019-11756、CNVD-2019-11757）。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-2019-11751

http://www.cnvd.org.cn/flaw/show/CNVD-2019-11750

http://www.cnvd.org.cn/flaw/show/CNVD-2019-11753

http://www.cnvd.org.cn/flaw/show/CNVD-2019-11752

http://www.cnvd.org.cn/flaw/show/CNVD-2019-11755

http://www.cnvd.org.cn/flaw/show/CNVD-2019-11754

http://www.cnvd.org.cn/flaw/show/CNVD-2019-11756

http://www.cnvd.org.cn/flaw/show/CNVD-2019-11757

3、Adobe 产品安全漏洞

Adobe Bridge 是一款免费数字资产管理应用程序。Adobe Reader(也被称为 Acrobat Reader)是一款 PDF 文件阅读软件。Adobe Acrobat 是一款 PDF 编辑软件。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞获取信息，远程代码执行。

CNVD 收录的相关漏洞包括：Adobe Bridge CC 堆溢出漏洞、Adobe Bridge CC 越界写入漏洞、Adobe Acrobat 和 Reader 越界读取漏洞（CNVD-2019-12255、CNVD-2019-12256、CNVD-2019-12257、CNVD-2019-12258、CNVD-2019-12259、CNVD-2019-12260）。其中，除“Adobe Bridge CC 堆溢出漏洞、Adobe Bridge CC 越界写入漏洞”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-2019-12183

http://www.cnvd.org.cn/flaw/show/CNVD-2019-12184

http://www.cnvd.org.cn/flaw/show/CNVD-2019-12255

http://www.cnvd.org.cn/flaw/show/CNVD-2019-12256

http://www.cnvd.org.cn/flaw/show/CNVD-2019-12257

http://www.cnvd.org.cn/flaw/show/CNVD-2019-12258

http://www.cnvd.org.cn/flaw/show/CNVD-2019-12259

http://www.cnvd.org.cn/flaw/show/CNVD-2019-12260

4、Cybozu 产品安全漏洞

Cybozu Garoon 是一套门户型 OA 办公系统。该系统提供门户、E-mail、书签、日程安排、公告栏、文件管理等功能。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，被重定向到任意网站，执行客户端代码等。

CNVD 收录的相关漏洞包括：Cybozu Garoon 开放重定向漏洞（CNVD-2019-12693）、Cybozu Garoon 跨站脚本漏洞（CNVD-2019-12692、CNVD-2019-12694、CNVD-2019-12699、CNVD-2019-12700、CNVD-2019-12702、CNVD-2019-12706）、Cybozu Garoon 输入验证错误漏洞。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-2019-12693

http://www.cnvd.org.cn/flaw/show/CNVD-2019-12692

http://www.cnvd.org.cn/flaw/show/CNVD-2019-12694

http://www.cnvd.org.cn/flaw/show/CNVD-2019-12699

http://www.cnvd.org.cn/flaw/show/CNVD-2019-12700

http://www.cnvd.org.cn/flaw/show/CNVD-2019-12702

http://www.cnvd.org.cn/flaw/show/CNVD-2019-12706

http://www.cnvd.org.cn/flaw/show/CNVD-2019-12711

5、libpng 'png_image_free'函数内存错误引用漏洞

libpng 是一个可对 PNG 图形文件实现创建、读写等操作的 PNG 参考库。libpng 被披露存在内存错误引用漏洞。攻击者可借助特制的文件利用该漏洞造成拒绝服务。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-2019-11838

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-2019-12135	Foxit Studio Photo 远程代码执行漏洞（CNVD-2019-12135）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://www.foxitsoftware.com/support/security-bulletins.php
CNVD-201	Nagios IM SQL 注入漏洞	高	厂商已发布漏洞修复程序，请及时关

9-12144			注更新：https://www.nagios.com/products/security/
CNVD-2019-12150	RubyGems 代码执行漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://www.ruby-lang.org/en/news/2019/03/05/multiple-vulnerabilities-in-rubygems/
CNVD-2019-12164	Kibana 命令注入漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://discuss.elastic.co/t/elastic-stack-6-6-1-and-5-6-15-security-update/169077
CNVD-2019-12467	IBM Content Navigator输入验证错误漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www-01.ibm.com/support/docview.wss?uid=ibm10880591
CNVD-2019-12470	Xiaomi Mi6 Browser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：https://www.mi.com/
CNVD-2019-12477	eVisitorPass 权限提升漏洞（CNVD-2019-12477）	高	厂商已发布漏洞修复程序，请及时关注更新：http://support.evisitorpass.com/Release_Notes.html
CNVD-2019-12479	rdesktop 输入验证错误漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/rdesktop/rdesktop/commit/4dca546d04321a610c1835010b5dad85163b65e1
CNVD-2019-12512	Grandstream GXP16xx 权限提升漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：http://www.grandstream.com/support/firmware
CNVD-2019-12522	PuTTY 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.chiark.greenend.org.uk/~sgtatham/putty/changes.html

小结：本周，Apple 被披露存在多个漏洞，攻击者可利用漏洞获取信息，以内核权限执行任意代码。此外，Oracle、Adobe、Cybozu 等多款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，被重定向到任意网站，执行客户端代码，造成拒绝服务等。libpng 被披露存在内存错误引用漏洞。攻击者可借助特制的文件利用该漏洞造成拒绝服务。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、Laravel SQL 注入漏洞

验证描述

Laravel Framework 是 Taylor Otwell 软件开发者开发的一款基于 PHP 的 Web 应用程序开发框架。

Laravel 5.4.15 版本中的 save.php 文件存在 SQL 注入漏洞。远程攻击者可借助‘dhx_user’和‘dhx_version’参数利用该漏洞执行任意的 SQL 命令。

验证信息

POC 链接：http://www.itblog.gbonanno.de/cve-2018-6330-laravel-sql-injection/

参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2019-12117

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. iLnkP2P 弱点暴露数百万物联网设备

一家深圳公司（该公司网站基本不更新）开发的软件 iLnkP2P 被发现存在严重安全漏洞，全世界有数百万物联网设备受到影响。iLnkP2P 被广泛用于安全摄像头和网络摄像头、婴儿监视器、智能门铃和数字录像机，它允许用户从任何地方简单快捷的访问设备。用户只需要下载移动应用，扫描设备上的二维码或六位数 ID。

安全研究员发现， iLnkP2P 设备没有提供任何验证或加密，很容易被枚举破解，允许攻击者与这些联网设备建立直接连接，绕过防火墙的限制。全世界有 200 多万物联网设备存在该漏洞，其中 39%位于中国，19%位于欧洲，还有 7%在美国。几乎半数存在漏洞的设备是海芯威视生产的，它的设备 ID 使用了前缀 FFFF、GGGG、HHHH、IIII、MMMM 和 ZZZZ。

参考链接：https://krebsonsecurity.com/2019/04/p2p-weakness-exposes-millions-of-iot-devices/

2. jQuery 原型污染漏洞分析和修复建议（CVE-2019-11358）

近日，jQuery 官方于发布安全预警通告，通报了漏洞编号为 CVE-2019-11358 的原型污染漏洞。由攻击者控制的属性可被注入对象，之后或经由触发 JavaScript 异常引发拒绝服务，或篡改该应用程序源代码从而强制执行攻击者注入的代码路径。

参考链接：https://www.freebuf.com/vuls/201762.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