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 29 日-2019 年 05 月 12 日　　2019 年第 18、19 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 277 个，其中高危漏洞 78 个、中危漏洞 182 个、低危漏洞 17 个。漏洞平均分值为 5.63。本周收录的漏洞中，涉及 0day 漏洞 136 个（占 49%），其中互联网上出现“TP-Link WDR Series 命令注入漏洞、CyberArk Software CyberArk Endpoint Privilege Manager 访问绕过漏洞”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 3387 与上周（2245 个）环比增长 51%。

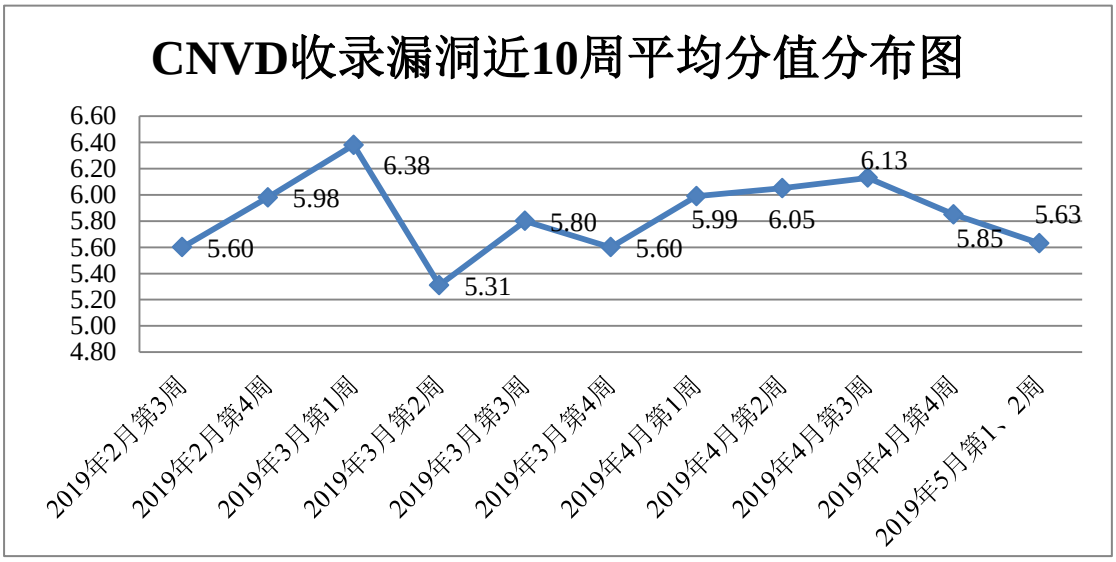

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 7 起，向银行、保险、能源等重要行业单位通报漏洞事件 44 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 478 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 24 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：

深圳出版集团有限公司、北京世纪长秋科技有限公司、北京东云创达科技有限公司、同方知网（北京）技术有限公司行业公司农业食品分社、深圳市显控科技股份有限公司、苏州汇川技术有限公司、哈尔滨新中新电子股份有限公司、江苏国泰新点软件有限公司、台州精迅信息技术有限公司、锐捷网络股份有限公司、北京神州数码云科信息技术有限公司、北京五指互联科技有限公司、北京火绒网络科技有限公司、重庆维普资讯有限公司、四川思途智旅软件有限公司、天津神州浩天科技有限公司、北京金方时代科技有限公司、湖南翱云网络科技有限公司、台湾永宏电机股份有限公司、北京山石网科信息技术有限公司、郑州路之易科技有限公司、深圳市英威腾电气股份有限公司、广州红帆科技有限公司、山西牛酷信息科技有限公司、厦门易尔通网络科技有限公司、深圳搜豹网络有限公司、国晋信息科技有限公司、上海岱牧网络有限公司、深圳个人数据管理服务有限公司、台安科技（无锡）有限公司、苏州烟火网络科技有限公司、永中软件股份有限公司、中铁二局集团新运工程有限公司、杭州帕拉迪网络科技有限公司、上海商创网络科技有限公司、沈阳盘古网络技术有限公司、北京中科网威信息技术有限公司、中交第二航务工程局有限公司、北京图灵开物技术有限公司、灵宝简好网络科技有限公司、成都华迈通信技术有限公司、微软(中国)有限公司、北京超星公司、辽宁民生智能仪表有限公司、太原迅易科技有限公司、哈尔滨巨耀网络科技有限公司、广州齐博网络科技有限公司、湖北中亿嘉讯传媒有限公司、湖南翱云网络科技有限公司、乐星产电(无锡)有限公司、深圳市显控科技股份有限公司、酷溜网（北京）科技有限公司、厦门美柚信息科技有限公司、成都天睿信息技术有限公司、湖南心艾网络科技有限公司、中华民国生物奥林匹亚委员会、和利时集团、中华民族图书馆、巨好用、鼎峰互动、雷风影视、飞飞影视导航系统（FeiFeiCms）、贴心猫(imcat)、壹凯巴 cms、第一工作室、兔兔影视、施耐德（Schneider Electric）、树洞外链、飞飞影视导航系统、爱客影院、爱客 CMS、优客 365、zzzcms、TP3-CMS、PassFab、Magneto Software、CSZ-CMS、BigTree CMS、Hongcms。

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、华为技术有限公司、深信服科技股份有限公司、新华三技术有限公司等单位报送公开收集的漏洞数量较多。任子行网络技术股份有限公司、长春嘉诚信息技术股份有限公司、国瑞数码零点实验室、内蒙古奥创科技有限公司、安徽锋刃信息科技有限公司、北京圣博润高新技术股份有限公司、中新网络信息安全股份有限公司、

上海银基信息安全技术股份有限公司、山东云天安全技术有限公司、泰山信息科技有限公司、山东华鲁科技发展股份有限公司、南京联成科技发展股份有限公司、上海并擎软件科技有限公司、四川虹微技术有限公司（子午攻防实验室）、河南信安世纪科技有限公司、中金金融认证中心有限公司、山石网科通信技术股份有限公司、新疆海狼科技有限公司、河北华测信息技术有限公司、北京信联科汇科技有限公司、连连银通电子支付有限公司、深圳个人数据管理服务有限公司及其他个人白帽子向 CNVD 提交了 3387 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 2332 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）	1802	1802
北京天融信网络安全技术有限公司	555	5
360 网神（补天平台）	530	530
哈尔滨安天科技集团股份有限公司	247	0
华为技术有限公司	177	0
深信服科技股份有限公司	140	0
新华三技术有限公司	122	0
北京启明星辰信息安全技术有限公司	93	0
四川无声信息技术有限公司	74	74
北京神州绿盟科技有限公司	48	10
中国电信集团系统集成有限责任公司	44	0
北京数字观星科技有限公司	39	0
恒安嘉新(北京)科技股份公司	21	2
厦门服云信息科技有限公司	12	0
北京知道创宇信息技术有限公司	4	0
南京铱迅信息技术股份有	1	1

限公司		
西安四叶草信息技术有限公司	1	1
任子行网络技术股份有限公司	146	146
长春嘉诚信息技术股份有限公司	118	118
国瑞数码零点实验室	78	78
内蒙古奥创科技有限公司	40	40
安徽锋刃信息科技有限公司	35	35
北京圣博润高新技术股份有限公司	34	34
中新网络信息安全股份有限公司	34	34
上海银基信息安全技术股份有限公司	23	23
山东云天安全技术有限公司	19	19
泰山信息科技有限公司	15	15
山东华鲁科技发展股份有限公司	10	10
南京联成科技发展股份有限公司	8	8
上海并擎软件科技有限公司	7	7
四川虹微技术有限公司（子午攻防实验室）	5	5
河南信安世纪科技有限公司	4	4
中金金融认证中心有限公司	4	4
山石网科通信技术股份有限公司	2	2
新疆海狼科技有限公司	2	2
河北华测信息技术有限公司	1	1
北京信联科汇科技有限公司	1	1

连连银通电子支付有限公司	1	1
深圳个人数据管理服务有限公司	1	1
CNCERT 天津分中心	25	25
CNCERT 河北分中心	7	7
CNCERT 广西分中心	3	3
CNCERT 贵州分中心	3	3
CNCERT 吉林分中心	3	3
CNCERT 宁夏分中心	2	2
CNCERT 四川分中心	2	2
CNCERT 重庆分中心	2	2
CNCERT 浙江分中心	1	1
个人	326	326
报送总计	4872	3387

本周漏洞按类型和厂商统计

本周，CNVD 收录了 277 个漏洞。应用程序 141 个，WEB 应用 86 个，网络设备（交换机、路由器等网络端设备）33 个，操作系统 12 个，安全产品 4 个，智能设备（物联网终端设备）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	141
WEB 应用	86
网络设备（交换机、路由器等网络端设备）	33
操作系统	12
安全产品	4
智能设备（物联网终端设备）漏洞	1

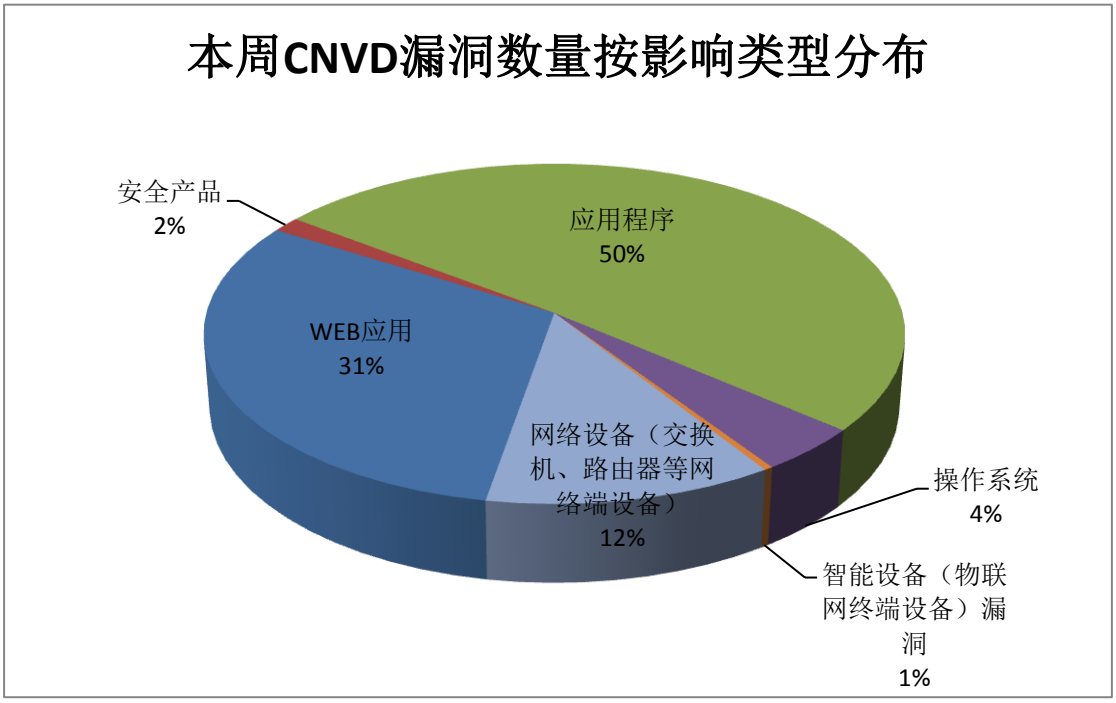

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Adobe、Google、IBM 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	Adobe	33	12%
2	Google	21	7%
3	IBM	11	4%
4	Sierra Wireless	8	3%
5	tecrail	7	3%
6	CloudBees	6	2%
7	D-Link	5	2%
8	PHP Scripts Mall	5	2%
9	UltraVNC	5	2%
10	其他	176	63%

本周行业漏洞收录情况

本周，CNVD 收录了 16 个电信行业漏洞，9 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，“Sierra Wireless AirLink ES450 未授权密码修改漏洞、Siemens Industrial Products with OPC UA 拒绝服务漏洞、Sierra Wireless AirLink ES450

操作系统命令注入漏洞”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/

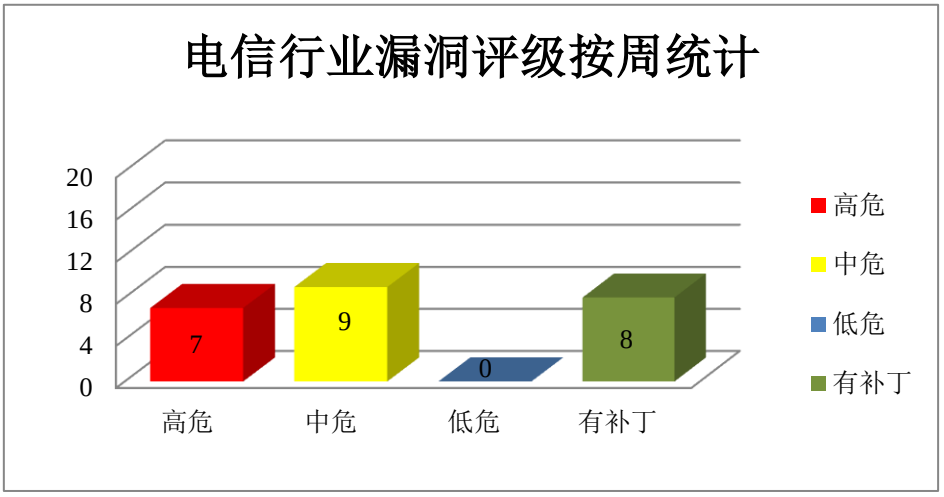

图 3 电信行业漏洞统计

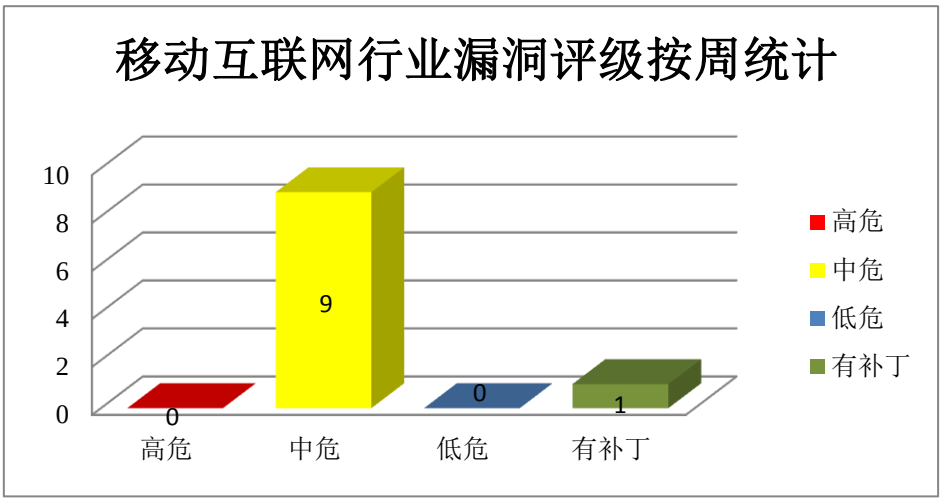

图 4 移动互联网行业漏洞统计

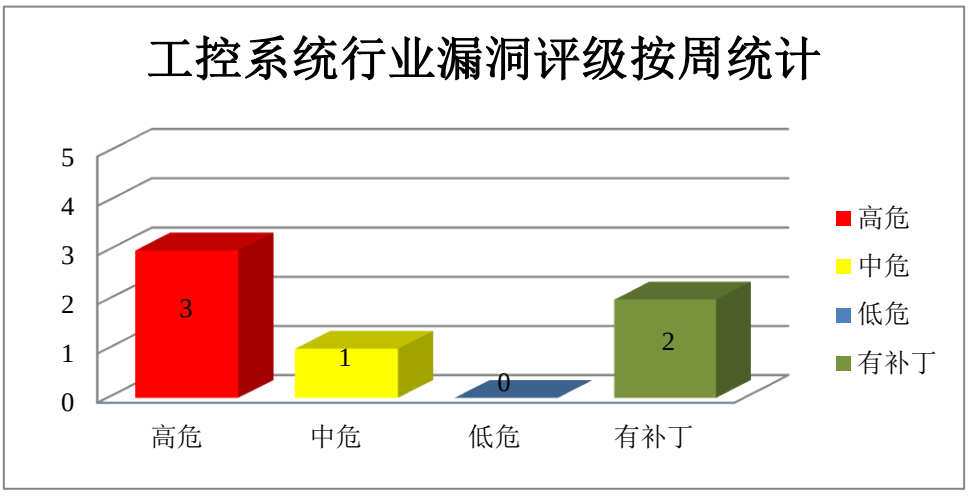

图 5 工控系统行业漏洞统计

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、Adobe 产品安全漏洞

Adobe Acrobat 是一款 PDF 编辑软件。Adobe Reader(也被称为 Acrobat Reader)是一款 PDF 文件阅读软件。本周，上述产品被披露存在堆溢出和越界读取漏洞，攻击者可利用漏洞获取信息，执行任意代码。

CNVD 收录的相关漏洞包括：Adobe Acrobat 和 Reader 堆溢出漏洞（CNVD-2019-12876、CNVD-2019-12878、CNVD-2019-12877）、Adobe Acrobat 和 Reader 越界读取漏洞（CNVD-2019-12879、CNVD-2019-12881、CNVD-2019-12880、CNVD-2019-12883、CNVD-2019-12882）。其中，“Adobe Acrobat 和 Reader 堆溢出漏洞（CNVD-2019-12876、CNVD-2019-12878、CNVD-2019-12877）”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-2019-12876
http://www.cnvd.org.cn/flaw/show/CNVD-2019-12878
http://www.cnvd.org.cn/flaw/show/CNVD-2019-12877
http://www.cnvd.org.cn/flaw/show/CNVD-2019-12879
http://www.cnvd.org.cn/flaw/show/CNVD-2019-12881
http://www.cnvd.org.cn/flaw/show/CNVD-2019-12880
http://www.cnvd.org.cn/flaw/show/CNVD-2019-12883
http://www.cnvd.org.cn/flaw/show/CNVD-2019-12882

2、Google 产品安全漏洞

Google Chrome 是一款 Web 浏览器。Android 是美国谷歌（Google）公司和开放手持设备联盟（简称 OHA）共同开发的一套以 Linux 为基础的开源操作系统。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞绕过 seccomp，提升权限，在系统上执行任意代码等。

CNVD 收录的相关漏洞包括：Google Android Broadcom 组件远程代码执行漏洞（CNVD-2019-13570）、Google Android seccomp 权限提升漏洞、Google Android NVIDIA Pixel C TrustZone 组件权限提升漏洞、Google Android System heap.cc 文件缓冲区溢出漏洞、Google Android System 缓冲区溢出漏洞、Google Android System 权限提升漏洞（CNVD-2019-13576）、Google Chrome V8 内存破坏漏洞（CNVD-2019-13583）、Google Chrome V8 越界读取漏洞（CNVD-2019-13585）。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-2019-13570

http://www.cnvd.org.cn/flaw/show/CNVD-2019-13572

http://www.cnvd.org.cn/flaw/show/CNVD-2019-13571

http://www.cnvd.org.cn/flaw/show/CNVD-2019-13574

http://www.cnvd.org.cn/flaw/show/CNVD-2019-13573

http://www.cnvd.org.cn/flaw/show/CNVD-2019-13576

http://www.cnvd.org.cn/flaw/show/CNVD-2019-13583

http://www.cnvd.org.cn/flaw/show/CNVD-2019-13585

3、IBM 产品安全漏洞

IBM Content Navigator 是美国 IBM 公司的一款 Web 客户机。IBM API Connect（APIConnect）是美国 IBM 公司的一套用于管理 API 生命周期的集成解决方案。IBM Jazz Reporting Service（JRS）是美国 IBM 公司的一套用于发现跨项目报表的应用程序。IBM Cúram Social Program Management（SPM）是美国 IBM 公司的一套社会计划管理解决方案。IBM TRIRIGA Application Platform 是美国 IBM 公司的一套用于部署 TRIRIGA 应用的技术平台。IBM Emptoris Contract Management 是美国 IBM 公司的一套可实现合同生命周期自动化的软件。IBM Business Process Manager 是一套综合的业务流程管理平台。IBM Business Automation Workflow 是一套工作流程自动化解决方案。IBM InfoSphere Information Server 是美国 IBM 公司的一套数据整合平台。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敏感信息，提升权限，执行客户端代码等。

CNVD 收录的相关漏洞包括：IBM Content Navigator 输入验证漏洞、IBM API Connect 信息泄露漏洞（CNVD-2019-12760）、IBM Jazz Reporting Service 跨站脚本漏洞（CNVD-2019-13241）、IBM Cúram Social Program Management 跨站请求伪造漏洞、IBM TRIRIGA Application Platform 信息泄露漏洞（CNVD-2019-13385）、IBM Emptoris Contract Management 信息泄露漏洞（CNVD-2019-13396）、IBM Business Automation Workflow 和 IBM Business Process Manager 信息泄露漏洞、IBM InfoSphere Information Server 提权漏洞。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-2019-12761

http://www.cnvd.org.cn/flaw/show/CNVD-2019-12760

http://www.cnvd.org.cn/flaw/show/CNVD-2019-13241

http://www.cnvd.org.cn/flaw/show/CNVD-2019-13257

http://www.cnvd.org.cn/flaw/show/CNVD-2019-13385

http://www.cnvd.org.cn/flaw/show/CNVD-2019-13396

http://www.cnvd.org.cn/flaw/show/CNVD-2019-13562

http://www.cnvd.org.cn/flaw/show/CNVD-2019-13768

4、Sierra Wireless 产品安全漏洞

Sierra Wireless AirLink ES450 是一款蜂窝网络调制解调器设备。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，执行未授权操作，执行非法命令等。

CNVD 收录的相关漏洞包括：Sierra Wireless AirLink ES450 未授权密码修改漏洞、Sierra Wireless AirLink ES450 操作系统命令注入漏洞、Sierra Wireless AirLink ES450 信息泄露漏洞（CNVD-2019-13240、CNVD-2019-13242、CNVD-2019-13397、CNVD-2019-13407、CNVD-2019-13408）、Sierra Wireless AirLink ES450 跨站请求伪造漏洞。其中，“Sierra Wireless AirLink ES450 未授权密码修改漏洞、Sierra Wireless AirLink ES450 操作系统命令注入漏洞”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-2019-13238

http://www.cnvd.org.cn/flaw/show/CNVD-2019-13239

http://www.cnvd.org.cn/flaw/show/CNVD-2019-13240

http://www.cnvd.org.cn/flaw/show/CNVD-2019-13242

http://www.cnvd.org.cn/flaw/show/CNVD-2019-13397

http://www.cnvd.org.cn/flaw/show/CNVD-2019-13406

http://www.cnvd.org.cn/flaw/show/CNVD-2019-13407

http://www.cnvd.org.cn/flaw/show/CNVD-2019-13408

5、D-Link DIR-878 缓冲区溢出漏洞

D-Link DIR-878 是一款无线路由器。D-Link DIR-878 被披露存在缓冲区溢出漏洞。远程攻击者可借助‘HNAP_AUTH’HTTP 报头利用该漏洞执行代码。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-2019-12893

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-2019-12757	CleanMyMac X 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：https://cleanmymac.com/
CNVD-2019-12886	Apache Mesos 代码执行漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://lists.apache.org/thread.html/b162

			dd624dc088cd634292f0402282a1d1d0ce853baeae8205bc033c@%3Cdev.mesos.apache.org%3E
CNVD-2019-12905	Siemens Industrial Products with OPC UA 拒绝服务漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.winccoa.com/news/detail/new-patch-p018-available-for-315.html
CNVD-2019-12916	Huawei AP4050DN-E 鉴权不当漏洞	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.huawei.com/cn/psirt/security-advisories/huawei-sa-20190327-01-ap-cn
CNVD-2019-13139	node-opencv 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://github.com/peterbraden/node-opencv
CNVD-2019-13248	Drupal 代码执行漏洞（CNVD-2019-13248）	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.drupal.org/sa-core-2019-005
CNVD-2019-13281	UltraVNC 堆缓冲区溢出漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://www.uvnc.com/
CNVD-2019-13383	dhcpcd 缓冲区溢出漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://roy.marples.name/archives/dhcpcd-discuss/0002428.html
CNVD-2019-13568	Gitea 远程代码执行漏洞（CNVD-2019-13568）	高	厂商已发布漏洞修复程序，请及时关注更新：https://github.com/go-gitea/gitea/releases/tag/v1.7.6；https://github.com/go-gitea/gitea/releases/tag/v1.8.0-rc3
CNVD-2019-13604	TP-Link EAP Controller for Linux 认证绕过漏洞	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.tp-link.com/en/download/EAP220.html#Controller_Software

小结：本周，Adobe 被披露存在堆溢出和越界读取漏洞，攻击者可利用漏洞获取信息，执行任意代码。此外，Google、IBM、Sierra Wireless 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，绕过 seccomp，提升权限，在系统上执行任意代码等。D-Link DIR-878 被披露存在缓冲区溢出漏洞。远程攻击者可借助‘HNAP_AUTH’ HTTP 报头利用该漏洞执行代码。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、TP-Link WDR Series 命令注入漏洞

验证描述

TP-Link WDR Series 是一款 WDR 系列无线路由器。

使用 v3 版本固件（例如：TL-WDR5620 V3.0 版本）的 TP-Link WDR Series 中存在命令注入漏洞，该漏洞源于‘citycode’字段中包含了 sehll 元字符。远程攻击者可利用该漏洞执行代码。

验证信息

POC 链接：https://github.com/afang5472/TP-Link-WDR-Router-Command-injection_POC/blob/master/poc.py

参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2019-13603

信息提供者

北京天融信网络安全技术有限公司

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. 英特尔固件引导验证绕过攻击

在荷兰阿姆斯特丹举行的 Hack in the Box 会议上，安全研究员演示了对英特尔 UEFI 参照实现的新攻击。这种攻击需要物理访问硬件，允许攻击者通过替换含有恶意代码的 SPI 闪存芯片，获得系统的完全的持久的访问权限。这种攻击不太可能成为普遍的危险，但显然可以被情报机构等特殊部门用于设置底层后门发动针对性的攻击。英特尔已经发布了补丁，但给 UEFI 打补丁并不是一件简单的事情。

参考链接：https://www.solidot.org/story?sid=60578

2. 研究人员发现隐藏在 Microsoft exchange 中的后门

研究人员发现 Microsoft Exchange 存在后门，可以利用被入侵的邮件服务器读取、修改或屏蔽邮件，甚至制作并发送新的邮件。此外，利用这个后门还能修改收件人、发件人、替换附件，甚至重新创建或重新发送邮件以绕过垃圾邮件过滤机制。该研究人员将这个后门命名为 LightNeuron，是首个利用恶意 Microsoft Exchange Transport Agent 发起攻击的后门。

参考链接：https://www.helpnetsecurity.com/2019/05/07/microsoft-exchange-backdoor/

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