国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2019 年 07 月 15 日-2019 年 07 月 21 日 **2019 年第 29 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 417 个，其中高危漏洞 137 个、中危漏洞 252 个、低危漏洞 28 个。漏洞平均分值为 6.05。本周收录的漏洞中，涉及 0day 漏洞 144 个（占 35%），其中互联网上出现“TP-Link Archer C1200 缓冲区溢出漏洞、MyBB JN-Jones MyBB-2FA 插件跨站请求伪造漏洞”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 3226 个，与上周（2528 个）环比增长 28%。

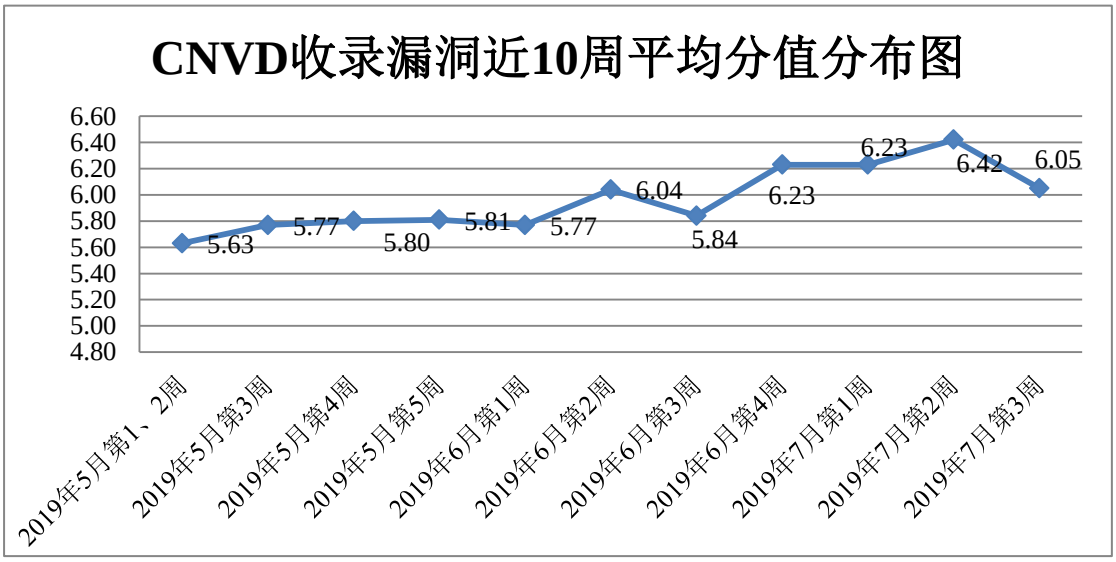

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 13 起，向银行、保险、能源等重要行业单位通报漏洞事件 11 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 333 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 65 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9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：

广州搜客网络科技有限公司、艾康 (上海) 信息技术有限公司、武汉类森科技有限公司、安阳智道传媒有限公司、盘古网络技术有限公司、桂林崇胜网络科技有限公司、中国重型汽车集团有限公司、山西牛酷信息科技有限公司、西安利友科技有限公司、济南有人物联网技术有限公司、中山市诺曼底信息科技有限公司、淄博闪灵网络科技有限公司、嘉兴想天信息科技有限公司、厦门凤凰创壹软件有限公司、广州市佰维网络科技有限公司、河南利梭互联网信息技术有限公司、佛山市云迈电子商务有限公司、苏州烟火网络科技有限公司、湖北亿百天信息技术有限公司、聊城博达网络科技有限公司、正方软件股份有限公司、上海美橙科技信息发展有限公司、北京珑大钜商科技有限公司、湖南强智科技发展有限公司、深圳市有方科技股份有限公司、上海域格信息技术有限公司、厦门四信通信科技有限公司、龙尚科技(上海)有限公司、珠海许继电气有限公司、青汗顺达科技有限公司、小米科技有限责任公司、北京云创联合科技有限公司 、浙江齐治科技股份有限公司、北京聚源百成网络科技有限公司、浙江逆天网络科技有限责任公司、中铁一局集团有限公司、上海待迩信息科技有限公司、升腾资讯有限公司、得实信息科技有限公司、中铁十七局集团第二工程有限公司、哈尔滨优阳科技有限公司、武汉烽火众智数字技术有限责任公司、成都康菲顿特网络科技有限公司、网展科技、乐清翰珂网络、中国铁路招标采购网、中国电工网、中国社会扶贫网、团啊网、中新传媒网、中国电子工业标准化技术协会社会责任工作委员会、中国岩石力学与工程学会、袁志蒙工作室、莱阳洪元电子商务科技工作室、中国网 •东海资讯、广州市群众体育指导中心、信呼、飞飞影视导航系统、施耐德（Schneider Electric）、海洋 CMS、ZBlogger 社区、PHPEMS、SemCms、GraphicsMagick Group 和 UQCMS。

本周，CNVD 发布了《Oracle 发布 2019 年 7 月的安全公告》。详情参见 CNVD 网站公告内容。

https://www.cnvd.org.cn/webinfo/show/5127

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，哈尔滨安天科技集团股份有限公司、华为技术有限公司、北京天融信网络安全技术有限公司、新华三技术有限公司、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。国瑞数码零点实验室、北京铭图天成信息技术有限公司、国网思极检测技术（北京）有限公司、南京众智维信息科技有限公司、山东云天安全技术有限公司、内蒙古奥创科技有限公司、任子行网络技术股份有限公司、山东新潮信息技术有限公司、广州锦行网络科技有限公司、山石网科通信技术有限公司、

北京圣博润高新技术股份有限公司、长春嘉诚信息技术股份有限公司、上海观安信息技术股份有限公司、山东华鲁科技发展股份有限公司、北京智游网安科技有限公司、厦门靠谱云股份有限公司、上海银基信息安全技术股份有限公司、连连银通电子支付有限公司、赛尔网络有限公司山东分公司、中移（杭州）信息技术有限公司及其他个人白帽子向 CNVD 提交了 3226 个以事件型漏洞为主的原创漏洞，其中包括奇安信网神（补天平台）和斗象科技（漏洞盒子）向 CNVD 共享的白帽子报送的 2524 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）	2072	2072
奇安信网神（补天平台）	452	452
哈尔滨安天科技集团股份有限公司	225	0
华为技术有限公司	156	0
北京天融信网络安全技术有限公司	134	2
新华三技术有限公司	120	0
深信服科技股份有限公司	83	0
北京神州绿盟科技有限公司	60	1
中国电信集团系统集成有限责任公司	46	0
中新网络信息安全股份有限公司	43	43
恒安嘉新(北京)科技股份公司	39	1
厦门服云信息科技有限公司	38	0
北京数字观星科技有限公司	14	0
四川无声信息技术有限公司	9	9
北京知道创宇信息技术股份有限公司	2	0
南京联成科技发展股份有限公司	1	1
国瑞数码零点实验室	136	136

北京铭图天成信息技术有限公司	55	55
国网思极检测技术（北京）有限公司	53	53
南京众智维信息科技有限公司	43	43
山东云天安全技术有限公司	39	39
内蒙古奥创科技有限公司	25	25
任子行网络技术股份有限公司	25	25
山东新潮信息技术有限公司	25	25
广州锦行网络科技有限公司	19	19
山石网科通信技术有限公司	14	14
北京圣博润高新技术股份有限公司	8	8
长春嘉诚信息技术股份有限公司	8	8
上海观安信息技术股份有限公司	6	6
山东华鲁科技发展股份有限公司	5	5
北京智游网安科技有限公司	3	3
厦门靠谱云股份有限公司	3	3
上海银基信息安全技术股份有限公司	3	3
连连银通电子支付有限公司	1	1
赛尔网络有限公司山东分公司	1	1
中移（杭州）信息技术有限公司	1	1
CNCERT 天津分中心	4	4
CNCERT 河北分中心	3	3
CNCERT 西藏分中心	3	3

CNCERT 贵州分中心	1	1
CNCERT 海南分中心	1	1
CNCERT 浙江分中心	1	1
个人	159	159
报送总计	4139	3226

本周漏洞按类型和厂商统计

本周，CNVD 收录了 417 个漏洞。应用程序 253 个，WEB 应用 67 个，网络设备（交换机、路由器等网络端设备）43 个，操作系统 31 个，数据库 9 个，安全产品 8 个，智能设备（物联网终端设备）6 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	253
WEB 应用	67
网络设备（交换机、路由器等网络端设备）	43
操作系统	31
数据库	9
安全产品	8
智能设备（物联网终端设备）	6

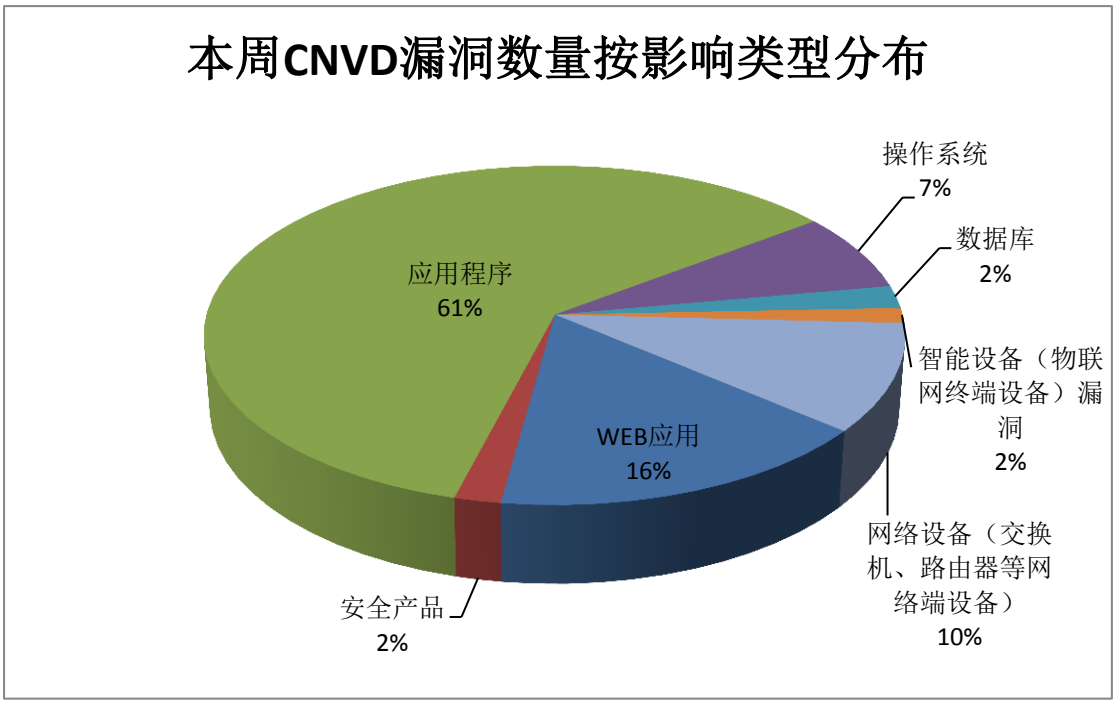

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Google、Adobe、D-Link 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	Google	54	13%
2	Adobe	46	11%
3	D-Link	17	4%
4	Mozilla	14	4%
5	HP	11	3%
6	CloudBees	10	2%
7	MacPaw	10	2%
8	Micro Focus	10	2%
9	Oracle	8	2%
10	其他	237	57%

本周行业漏洞收录情况

本周，CNVD 收录了 16 个电信行业漏洞，21 个移动互联网行业漏洞，3 个工控行业漏洞（如下图所示）。其中，“Google Android Media framework 远程代码执行漏洞（CNVD-2019-23123）、SolarWinds Network Performance Monitor SQL 注入漏洞、Linksys E1200 和 E2500 操作系统命令注入漏洞、Google Android System 权限提升漏洞（CNVD-2019-23099）”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/

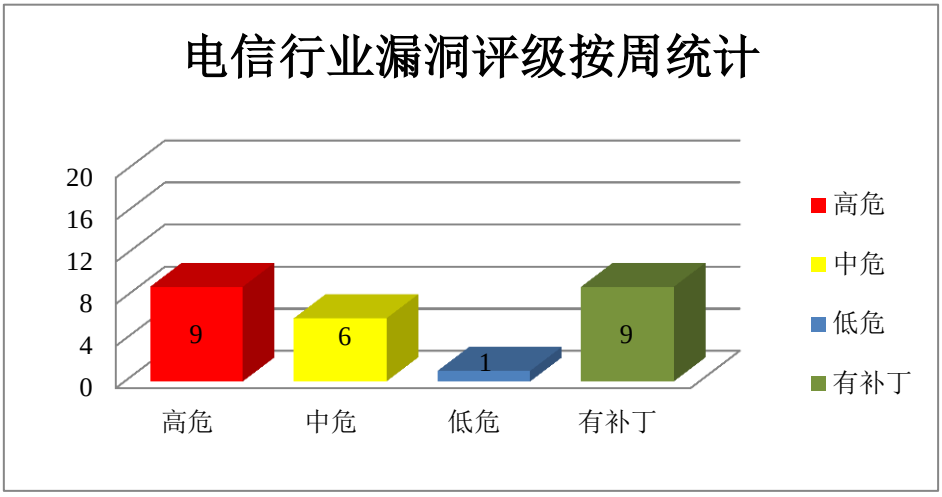

图 3 电信行业漏洞统计

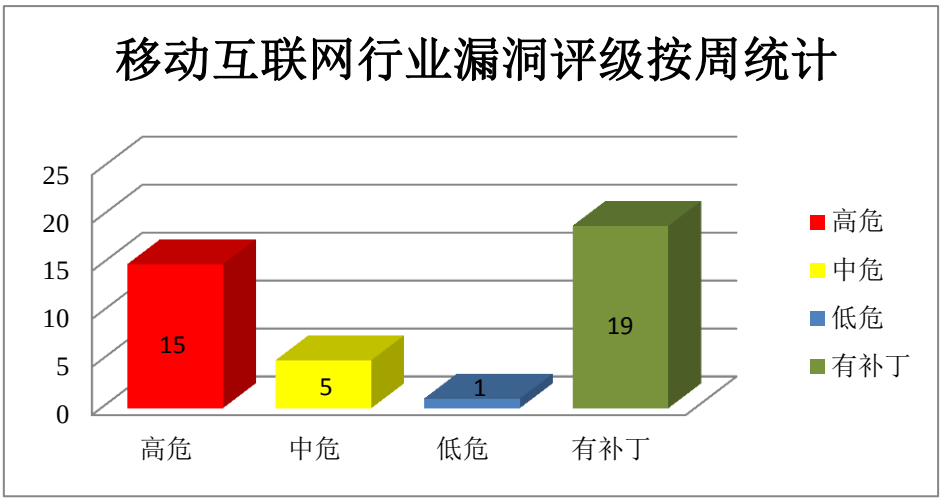

图 4 移动互联网行业漏洞统计

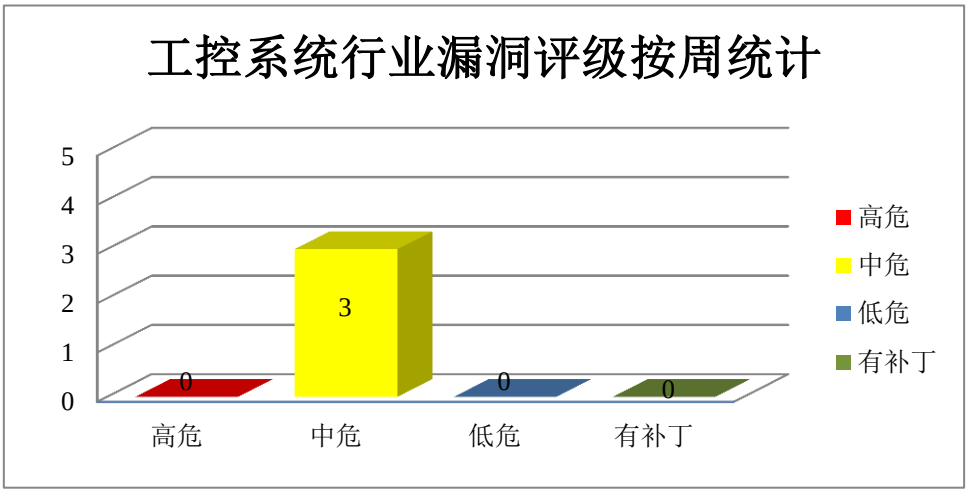

图 5 工控系统行业漏洞统计

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、Google 产品安全漏洞

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权限提升漏洞，攻击者可利用漏洞提升权限。

CNVD 收录的相关漏洞包括：Google Android Framework 权限提升漏洞（CNVD-2019-23120、CNVD-2019-23121）、Google Android System 权限提升漏洞（CNVD-2019-23099、CNVD-2019-23100、CNVD-2019-23320、CNVD-2019-23321、CNVD-2019-23322、CNVD-2019-23323）。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-2019-23120
http://www.cnvd.org.cn/flaw/show/CNVD-2019-23121
http://www.cnvd.org.cn/flaw/show/CNVD-2019-23099
http://www.cnvd.org.cn/flaw/show/CNVD-2019-23100
http://www.cnvd.org.cn/flaw/show/CNVD-2019-23320
http://www.cnvd.org.cn/flaw/show/CNVD-2019-23321
http://www.cnvd.org.cn/flaw/show/CNVD-2019-23322
http://www.cnvd.org.cn/flaw/show/CNVD-2019-23323

2、Adobe 产品安全漏洞

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，该产品被披露存在内存错误引用漏洞，攻击者可利用漏洞执行任意代码。

CNVD 收录的相关漏洞包括：Adobe Acrobat/Reader 内存错误引用漏洞（CNVD-2019-22787、CNVD-2019-22788、CNVD-2019-22791、CNVD-2019-22789、CNVD-2019-22790、CNVD-2019-22792、CNVD-2019-22793、CNVD-2019-22794）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-2019-22787
http://www.cnvd.org.cn/flaw/show/CNVD-2019-22788
http://www.cnvd.org.cn/flaw/show/CNVD-2019-22791
http://www.cnvd.org.cn/flaw/show/CNVD-2019-22789
http://www.cnvd.org.cn/flaw/show/CNVD-2019-22790
http://www.cnvd.org.cn/flaw/show/CNVD-2019-22792
http://www.cnvd.org.cn/flaw/show/CNVD-2019-22793
http://www.cnvd.org.cn/flaw/show/CNVD-2019-22794

3、Mozilla 产品安全漏洞

Mozilla Firefox 是一款开源 Web 浏览器。Mozilla Firefox ESR 是 Firefox(Web 浏览器)的一个延长支持版本。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安全限制，获取敏感信息，执行任意代码，发起拒绝服务攻击等。

CNVD 收录的相关漏洞包括：Mozilla Firefox 信息泄露漏洞（CNVD-2019-22627）、Mozilla Firefox 安全绕过漏洞（CNVD-2019-22628）、Mozilla Firefox 拒绝服务漏洞（CNVD-2019-22629）、Mozilla Firefox 内存错误引用漏洞（CNVD-2019-22632）、Mozilla Firefox 和 Firefox ESR 安全绕过漏洞（CNVD-2019-22851）、Mozilla Firefox 和 Firefox ESR 内存破坏漏洞（CNVD-2019-22854）、Mozilla Firefox 和 Firefox ESR 任意代码执行漏洞（CNVD-2019-22855）、Mozilla Firefox 和 Firefox ESR 拒绝服务漏洞（ CNVD-2019-22852）。其中，“Mozilla Firefox 和 Firefox ESR 内存破坏漏洞（CNVD-2019-22854）、Mozilla Firefox 和 Firefox ESR 任意代码执行漏洞（CNVD-2019-22855）”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-2019-22627
http://www.cnvd.org.cn/flaw/show/CNVD-2019-22628
http://www.cnvd.org.cn/flaw/show/CNVD-2019-22629
http://www.cnvd.org.cn/flaw/show/CNVD-2019-22632
http://www.cnvd.org.cn/flaw/show/CNVD-2019-22851
http://www.cnvd.org.cn/flaw/show/CNVD-2019-22854
http://www.cnvd.org.cn/flaw/show/CNVD-2019-22855
http://www.cnvd.org.cn/flaw/show/CNVD-2019-22852

4、CloudBees 产品安全漏洞

CloudBees Jenkins（Hudson Labs）是一套基于 Java 开发的持续集成工具。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，执行客户端代码等。

CNVD 收录的相关漏洞包括：CloudBees Jenkins ElectricFlow Plugin 信息泄露漏洞、CloudBees Jenkins ElectricFlow Plugin 跨站请求伪造漏洞、CloudBees Jenkins ElectricFlow Plugin 授权问题漏洞、CloudBees Jenkins Token Macro Plugin XML 外部实体漏洞、CloudBees Jenkins ElectricFlow Plugin 跨站脚本漏洞、CloudBees Jenkins JX Resources Plugin 信任管理问题漏洞、CloudBees Jenkins JX Resources Plugin 跨站请求伪造漏洞、CloudBees Jenkins 路径遍历漏洞（CNVD-2019-23290）。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-2019-22637
http://www.cnvd.org.cn/flaw/show/CNVD-2019-22638
http://www.cnvd.org.cn/flaw/show/CNVD-2019-22639

http://www.cnvd.org.cn/flaw/show/CNVD-2019-22647

http://www.cnvd.org.cn/flaw/show/CNVD-2019-22648

http://www.cnvd.org.cn/flaw/show/CNVD-2019-22653

http://www.cnvd.org.cn/flaw/show/CNVD-2019-22654

http://www.cnvd.org.cn/flaw/show/CNVD-2019-23290

5、D-Link DCS-1130 和 D-Link DCS-1100 缓冲区溢出漏洞

D-Link DCS-1100 和 D-Link DCS-1130 都是中国台湾友讯（D-Link）公司的一款网络摄像机。D-Link DCS-1100 和 DCS-1130 被披露存在缓冲区溢出漏洞。攻击者可通过攻击 orthrus 守护进程利用该漏洞完全控制设备，查看摄像头所拍摄的图像。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-2019-23332

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-2019-22482	Atlassian JIRA 模板注入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://confluence.atlassian.com/jira/jira-security-advisory-2019-07-10-973486595.html
CNVD-2019-22613	Micro Focus Filr 本地权限提升漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://download.novell.com/Download?buildid=nZUCSDkvpxk~
CNVD-2019-22780	Linksys E1200 和 E2500 操作系统命令注入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://talosintelligence.com/vulnerability_reports/TALOS-2018-0625
CNVD-2019-22782	SchedMD Slurm SQL 注入漏洞（CNVD-2019-22782）	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.schedmd.com/news.php?id=218
CNVD-2019-22864	uLaunchELF 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://github.com/AKuHAK/uLaunchELF/issues/14
CNVD-2019-23070	SolarWinds Network Performance Monitor SQL 注入漏洞	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.solarwinds.com/

CNVD-2019-23071	Palo Alto Networks PAN-OS 命令注入漏洞（CNVD-2019-23071）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://securityadvisories.paloaltonetworks.com/Home/Detail/156
CNVD-2019-23089	Moodle 跨站请求伪造漏洞（CNVD-2019-23089）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://moodle.org/mod/forum/discuss.php?d=388567
CNVD-2019-23306	HP Support Assistant 权限提升漏洞（CNVD-2019-23306）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://support.hp.com/us-en/document/c06388027
CNVD-2019-23346	ProClima 代码注入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.schneider-electric.com/en/product-range-download/2560-proclima/#tabs-top

小结：本周，Google 被披露存在权限提升漏洞，攻击者可利用漏洞提升权限。此外，Adobe、Mozilla、CloudBees 等多款产品被披露存在多个漏洞，攻击者可利用漏洞绕过安全限制，获取敏感信息，执行任意代码，发起拒绝服务攻击等。D-Link DCS-1130 和 D-Link DCS-1100 被披露存在缓冲区溢出漏洞。攻击者可通过攻击 orthrus 守护进程利用该漏洞完全控制设备，查看摄像头所拍摄的图像。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 Archer C1200 缓冲区溢出漏洞

验证描述

TP-Link Archer C1200 是中国普联（TP-Link）的一款无线路由器。

TP-Link Archer C1200 1.0.0 Build 20180502 rel.45702 及之前版本中的 TP-Link Device Debug 协议的 CMD_SET_CONFIG_COUNTRY 存在缓冲区溢出漏洞。该漏洞源于网络系统或产品在内存上执行操作时，未正确验证数据边界，导致向关联的其他内存位置上执行了错误的读写操作。攻击者可利用该漏洞导致缓冲区溢出或堆溢出等。

验证信息

POC 链接：https://fakhrizulkifli.github.io/posts/2019/07/15/CVE-2019-13614/

参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2019-23287

信息提供者

CNVD 工作组

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. Android 出现新漏洞，可在无权限的情况下利用传感器获取语音信息

网络安全团队发现了一种全新的旁路攻击，可以通过恶意程序窃听手机扬声器发出的声音，并且无需任何设备许可。这种新形式的攻击被称作 Spearphone，其原理是利用手机自带的运动传感器（也就是加速度计）实现对设备的无限制访问，由于这个功能是基于硬件的，内置于大多数 Android 设备中。因此，即使没有权限也可以通过设备上安装的任意应用程序对其进行访问。加速度计是一种运动传感器，通过测量速度相对于幅度或者方向的时间变化率，来让手机应用监控设备的运动状态，例如倾斜、摇晃、旋转或摆动等动作。

参考链接：https://www.freebuf.com/news/208700.html

2. 索尼 BRAVIA 智能电视存在漏洞

BRAVIA 是索尼视觉产品智能电视，是众所周知的高标准产品。BRAVIA 是日本索尼(Sony)在新一代的电视品牌。BRAVIA 是“Best Resolution Audio Visual Integrated Architecture”的缩写，代表“最高品质的影音整合架构”。XEN1THLabs 在 Sony 产品中发现了两个漏洞，并与索尼披露了这些安全缺陷。索尼 Bravia 智能电视中被发现存在安全性问题，但是索尼没有公布受影响型号的列表。

参考链接：https://www.freebuf.com/vuls/207968.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