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 22 日-2019 年 07 月 28 日 **2019 年第 30 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 443 个，其中高危漏洞 198 个、中危漏洞 181 个、低危漏洞 64 个。漏洞平均分值为 6.50。本周收录的漏洞中，涉及 0day 漏洞 107 个（占 24%），其中互联网上出现“Invoxia NVX220 信任管理问题漏洞、Private Internet Access (PIA) VPN 客户端任意代码执行漏洞（CNVD-2019-24214）”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 2259 个，与上周（3226 个）环比下降 30%。

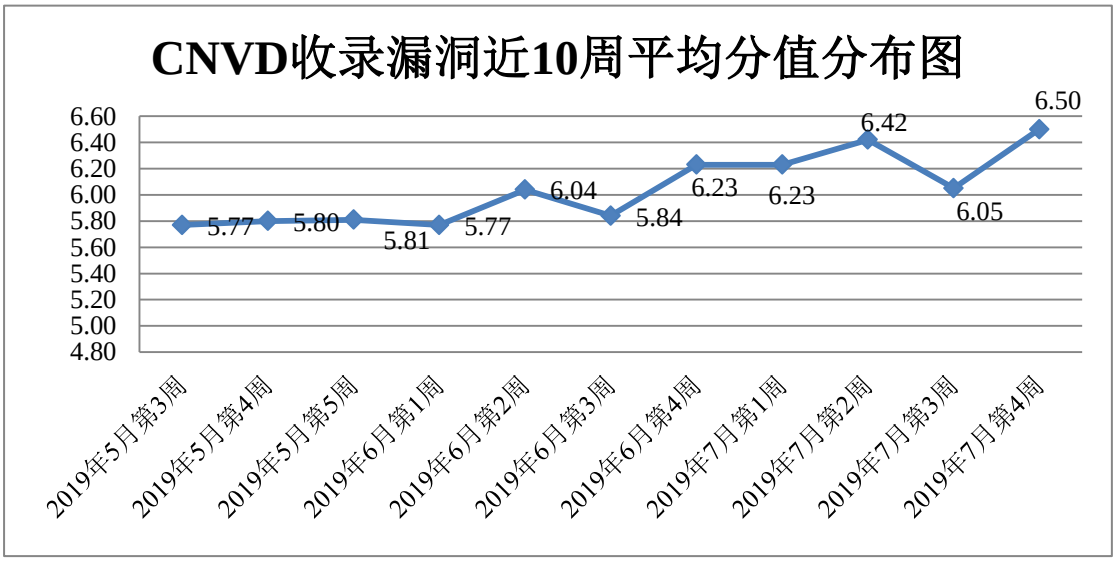

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 12 起，向银行、保险、能源等重要行业单位通报漏洞事件 34 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 437 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 32 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：

桂林崇胜网络科技有限公司、沧州市凡诺广告传媒有限公司、山石网科通信技术有限公司、山大鲁能信息科技有限公司、东莞偶偶网络科技有限公司、福建皮皮跳动科技有限公司、中山市华拓信息技术有限公司、北京五指互联科技有限公司、中海粮油集团有限公司、上海卓卓网络科技有限公司、深圳市锟锆科技有限公司、深圳市金卫信信息技术有限公司 、福建星网锐捷通讯股份有限公司、北京亿赛通科技发展有限责任公司、浙江大华技术股份有限公司、台州精迅信息技术有限公司、研华科技（中国）有限公司、深圳市贝尔利科技有限公司、中国生物技术股份有限公司、中国医药集团有限公司、上海同磊土木工程技术有限公司、深圳市金卫信信息技术有限公司、锐捷网络股份有限公司、山西牛酷信息科技有限公司、上海丹帆网络科技有限公司、北京盈算计算机系统工程有限公司、四川云百特科技有限公司、上海浪擎信息科技有限公司、江苏汇文软件有限公司、广州搜客网络科技有限公司、武汉达梦数据库有限公司、郑州维维信息技术有限公司、浙江齐治科技股份有限公司、中国船舶重工集团国际工程有限公司、深圳市硕赢互动信息技术有限公司、深圳搜豹网络有限公司、太原迅易科技有限公司、台达电子企业管理(上海)有限公司、北京卓正志远软件有限公司、深圳好生意网络工作室、国药控股北京华鸿有限公司、青岛圭谷品牌设计有限公司、杭州可道云网络有限公司、中国国际电视总公司、武汉客客信息技术有限公司、中泽国际会展（北京）有限公司、国药控股贵州有限公司、正方软件股份有限公司、海南赞赞网络科技有限公司、厦门科汛软件有限公司、昆山优网信息科技有限公司、郑州新开普电子技术有限公司、国药控股常州医药物流中心有限公司、中国医药保健品进出口商会、中国国际经济贸易仲裁委员会、中国自动化学会、中国质量协会、中国盲文出版社、中国数字认证网、六安市开发区鹏程网络工作室、CCTV 乡情快讯、Creatiwity 机构、UQCMS、OFCMS、ShopXO、ArtCMS、ShyPost、UPX、Zzzcms、SemCms、PHPEMS、ThinkSAAS、UCMS。

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、深信服科技股份有限公司、厦门服云信息科技有限公司、华为技术有限公司等单位报送公开收集的漏洞数量较多。山东新潮信息技术有限公司、南京众智维信息科技有限公司、国瑞数码零点实验室、国网思极检测技术（北京）有限公司、任子行网络技术股份有限公司、山东云天安全技术有限公司、长春嘉诚信息技术股份有限公司、内蒙古奥创科技有限公司、山东华鲁科技发展股份有限公司、北京铭图天成信息技术有限公司、山东新潮信息技术有限公司、河南信安世纪科技有限公司、山石网科

通信技术有限公司、北京智游网安科技有限公司、北京国腾创新科技有限公司、北京圣博润高新技术股份有限公司、上海并擎软件科技有限公司、上海物盾信息科技有限公司、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 2259 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 1561 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）	1127	1127
奇安信网神（补天平台）	434	434
北京天融信网络安全技术有限公司	382	12
哈尔滨安天科技集团股份有限公司	201	0
深信服科技股份有限公司	175	0
厦门服云信息科技有限公司	98	3
华为技术有限公司	83	0
中国电信集团系统集成有限责任公司	56	0
中新网络信息安全股份有限公司	56	56
新华三技术有限公司	50	0
北京神州绿盟科技有限公司	46	2
恒安嘉新(北京)科技股份公司	26	5
北京数字观星科技有限公司	14	0
南京联成科技发展股份有限公司	7	7
浙江大华技术股份有限公司	6	6
北京知道创宇信息技术股份有限公司	4	2
山东新潮信息技术有限公司	79	79

南京众智维信息科技有限公司	68	68
国瑞数码零点实验室	61	61
国网思极检测技术（北京）有限公司	34	34
任子行网络技术股份有限公司	24	24
山东云天安全技术有限公司	22	22
长春嘉诚信息技术股份有限公司	22	22
内蒙古奥创科技有限公司	19	19
山东华鲁科技发展股份有限公司	9	9
北京铭图天成信息技术有限公司	8	8
山东新潮信息技术有限公司	6	6
河南信安世纪科技有限公司	3	3
山石网科通信技术有限公司	3	3
北京智游网安科技有限公司	2	2
北京国腾创新科技有限公司	2	2
北京圣博润高新技术股份有限公司	1	1
上海并擎软件科技有限公司	1	1
上海物盾信息科技有限公司	1	1
中移（杭州）信息技术有限公司	1	1
CNCERT 宁夏分中心	9	9
CNCERT 海南分中心	6	6
CNCERT 河北分中心	2	2
CNCERT 天津分中心	2	2

CNCERT 内蒙古分中心	1	1
个人	219	219
报送总计	3370	2259

本周漏洞按类型和厂商统计

本周，CNVD 收录了 443 个漏洞。应用程序 291 个，WEB 应用 69 个，操作系统 47 个，网络设备（交换机、路由器等网络端设备）26 个，智能设备（物联网终端设备）5 个，安全产品 4 个，数据库 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	291
WEB 应用	69
操作系统	47
网络设备（交换机、路由器等网络端设备）	26
智能设备（物联网终端设备）	5
安全产品	4
数据库	1

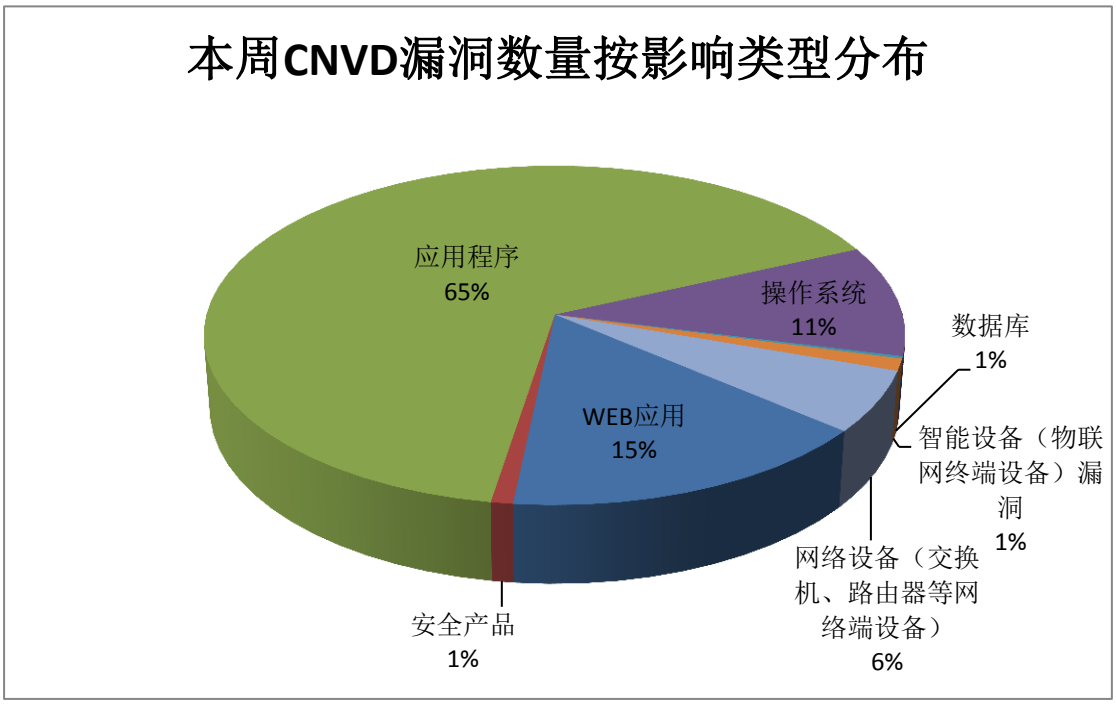

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 HP、Google、CloudBees 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	HP	90	20%
2	Google	54	13%
3	CloudBees	46	10%
4	Oracle	15	3%
5	JetBrains	13	3%
6	Zoho	13	3%
7	GitLab	10	2%
8	Moxa	10	2%
9	Juniper Networks	8	2%
10	其他	184	42%

本周行业漏洞收录情况

本周，CNVD 收录了 9 个电信行业漏洞，15 个移动互联网行业漏洞（如下图所示）。其中，“Cisco NX-OS Software 本地权限提升漏洞、ProFTPd 任意文件拷贝漏洞、Moxa OnCell G3100-HSPA 内存破坏漏洞、Google Android System 组件远程代码执行漏洞”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/

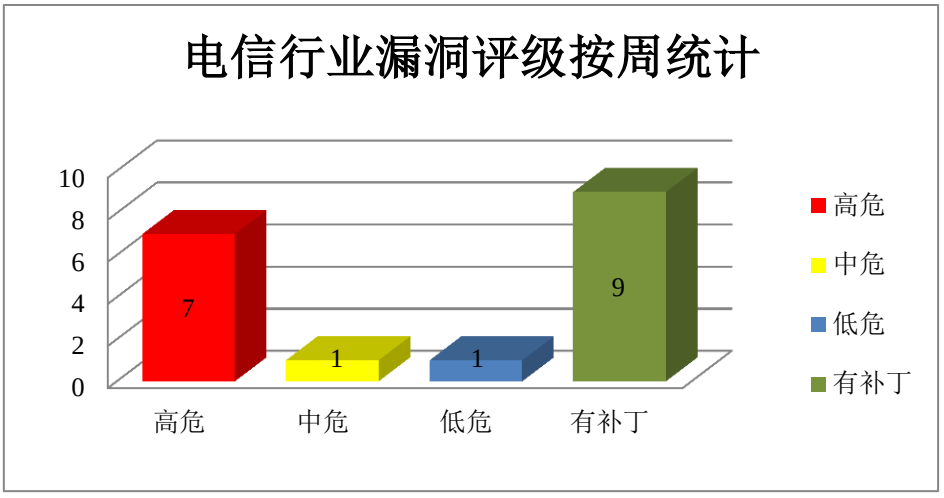

图 3 电信行业漏洞统计

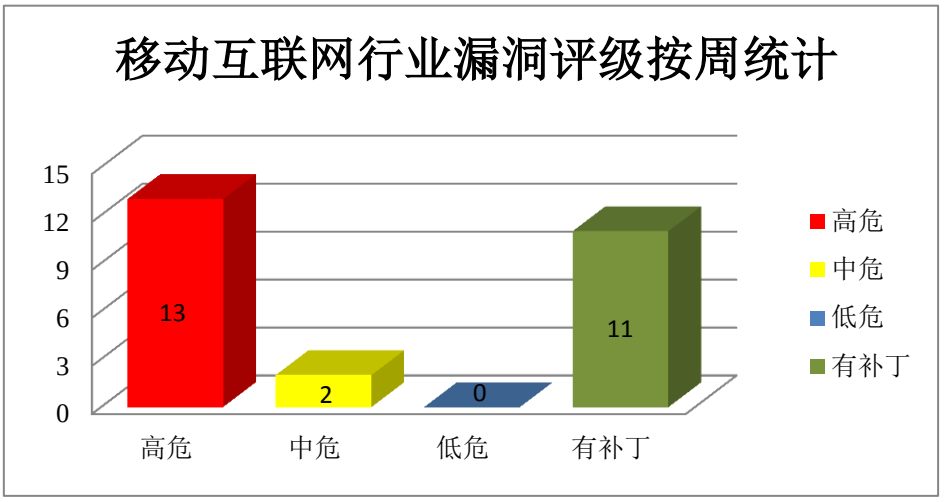

图 4 移动互联网行业漏洞统计

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、HP 产品安全漏洞

HPE Intelligent Management Center（IMC）是一个从底层构建的综合管理平台，支持故障、配置、记账、性能及安全（FCAPS）模型。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机制执行未授权操作，导致缓冲区溢出，执行远程代码，造成拒绝服务。

CNVD 收录的相关漏洞包括：HPE Intelligent Management Center (IMC)拒绝服务漏洞、HPE Intelligent Management Center (IMC) UrlAccessController 认证绕过漏洞、HPE Intelligent Management Center (IMC)远程代码执行漏洞（CNVD-2019-23771、CNVD-2019-23769、CNVD-2019-23770、CNVD-2019-23772、CNVD-2019-23773）、HPE Intelligent Management Center (IMC)栈缓冲区溢出漏洞（CNVD-2019-24023）。其中，除“HPE Intelligent Management Center (IMC)远程代码执行漏洞（CNVD-2019-23769）”外，其余漏洞的综合评级为“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-2019-23551

http://www.cnvd.org.cn/flaw/show/CNVD-2019-23760

http://www.cnvd.org.cn/flaw/show/CNVD-2019-23771

http://www.cnvd.org.cn/flaw/show/CNVD-2019-23769

http://www.cnvd.org.cn/flaw/show/CNVD-2019-23770

http://www.cnvd.org.cn/flaw/show/CNVD-2019-23772

http://www.cnvd.org.cn/flaw/show/CNVD-2019-23773

http://www.cnvd.org.cn/flaw/show/CNVD-2019-24023

2、CloudBees 产品安全漏洞

CloudBees Jenkins 是一套基于 Java 开发的持续集成工具，它主要用于监控持续的软件版本发布/测试项目和一些定时执行的任务。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，造成拒绝服务（无限循环）等。

CNVD 收录的相关漏洞包括：CloudBees Jenkins SSH Credentials Plugin 任意文件读取漏洞、CloudBees Jenkins SAML PluginHTTP 会话固定漏洞 、CloudBees jenkins-email-ext Email Extension 插件信息泄露漏洞、CloudBees Jenkins 拒绝服务漏洞（CNVD-2019-23809）、CloudBees Jenkins Cloud Foundry Plugin 信息泄露漏洞、CloudBees Jenkins JMS Messaging Plugin 服务器请求伪造漏洞、CloudBees Jenkins Script Security Plugin 沙盒绕过漏洞、CloudBees Jenkins 信息泄露漏洞（CNVD-2019-24407）。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-2019-23805
http://www.cnvd.org.cn/flaw/show/CNVD-2019-23806
http://www.cnvd.org.cn/flaw/show/CNVD-2019-23810
http://www.cnvd.org.cn/flaw/show/CNVD-2019-23809
http://www.cnvd.org.cn/flaw/show/CNVD-2019-23828
http://www.cnvd.org.cn/flaw/show/CNVD-2019-23832
http://www.cnvd.org.cn/flaw/show/CNVD-2019-23829
http://www.cnvd.org.cn/flaw/show/CNVD-2019-24407

3、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远程代码执行漏洞，攻击者可利用漏洞执行任意代码。

CNVD 收录的相关漏洞包括：Google Android Media framework 远程代码执行漏洞（CNVD-2019-23555、CNVD-2019-23556）、Google Android System 组件远程代码执行漏洞、Google Android Framework 组件远程代码执行漏洞（CNVD-2019-23561、CNVD-2019-23562、CNVD-2019-23563）、Google Android 远程代码执行漏洞（CNVD-2019-24161、CNVD-2019-24164）。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-2019-23555
http://www.cnvd.org.cn/flaw/show/CNVD-2019-23556
http://www.cnvd.org.cn/flaw/show/CNVD-2019-23560
http://www.cnvd.org.cn/flaw/show/CNVD-2019-23561

http://www.cnvd.org.cn/flaw/show/CNVD-2019-23562

http://www.cnvd.org.cn/flaw/show/CNVD-2019-23563

http://www.cnvd.org.cn/flaw/show/CNVD-2019-24161

http://www.cnvd.org.cn/flaw/show/CNVD-2019-24164

4、Moxa 产品安全漏洞

Moxa OnCell G3100-HSPA 是一款 G3100-HSPA 系列蜂窝网络网关设备。Moxa OnCell G3470A-LTE 是一款 G3470A-LTE 系列蜂窝网络网关设备。Moxa AWK-3121 是一款工业级无线访问接入点。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，破坏内存等。

CNVD 收录的相关漏洞包括：Moxa OnCell G3100-HSPA 安全绕过漏洞、Moxa OnCell G3100-HSPA 内存破坏漏洞（CNVD-2019-23543、CNVD-2019-23545）、Moxa OnCell G3470A-LTE 内存破坏漏洞（CNVD-2019-23546、CNVD-2019-23547）、Moxa OnCell G3100-HSPA 安全特征问题漏洞、Moxa AWK-3121 信息泄露漏洞、Moxa AWK-3121 加密问题漏洞。其中，除“Moxa OnCell G3100-HSPA 安全特征问题漏洞、Moxa AWK-3121 信息泄露漏洞、Moxa AWK-3121 加密问题漏洞”外，其余漏洞的综合评级为“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-2019-23541

http://www.cnvd.org.cn/flaw/show/CNVD-2019-23543

http://www.cnvd.org.cn/flaw/show/CNVD-2019-23546

http://www.cnvd.org.cn/flaw/show/CNVD-2019-23545

http://www.cnvd.org.cn/flaw/show/CNVD-2019-23544

http://www.cnvd.org.cn/flaw/show/CNVD-2019-23547

http://www.cnvd.org.cn/flaw/show/CNVD-2019-23548

http://www.cnvd.org.cn/flaw/show/CNVD-2019-23550

5、Sony BRAVIA Smart TVs 拒绝服务漏洞

Sony BRAVIA Smart TVs 是日本索尼（Sony）公司的一款智能电视。Sony BRAVIA Smart TVs 被披露存在拒绝服务漏洞。攻击者可利用该漏洞造成电视卡屏，无法响应，程序崩溃并且导致电视重启。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-2019-23992

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-201	Cybozu Remote Service 任意	高	厂商已发布了漏洞修复程序，请及时

9-23792	文件上传漏洞		关注更新：https://kb.cybozu.support/article/34311/
CNVD-2019-23994	FasterXML jackson-databind 远程命令执行漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://github.com/FasterXML/jackson-databind/commit/c9ef4a10d6f6633cf470d6a469514b68fa2be234
CNVD-2019-24149	Google Android Qualcomm 闭源组件缓冲区溢出漏洞（CNVD-2019-24149）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://source.android.com/security/bulletin/2019-04-01.html
CNVD-2019-24160	Cisco NX-OS Software 本地安全绕过漏洞	高	用户可联系供应商获得补丁信息：https://www.cisco.com/
CNVD-2019-24188	Google Android 缓冲区溢出漏洞（CNVD-2019-24188）	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.codeaurora.org/security-bulletin/2018/09/04/september-2018-code-aurora-security-bulletin
CNVD-2019-24192	Amcrest IPM-721S 授权问题漏洞	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://amcrest.com/
CNVD-2019-24231	JetBrains YouTrack server 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://blog.jetbrains.com/blog/2019/06/19/jetbrains-security-bulletin-q1-2019/
CNVD-2019-24248	ipswitch WS_FTP Server 路径遍历漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://docs.ipswitch.com/WS_FTP_Server2018/ReleaseNotes/index.htm#49242.htm
CNVD-2019-24390	Microsoft Team Foundation Server 和 Microsoft Azure DevOps Server 信息泄露漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0971
CNVD-2019-24547	Zoho ManageEngine ADSelfService Plus 认证绕过漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://www.manageengine.com/products/self-service-password/

小结：本周，HP 被披露存在多个漏洞，攻击者可利用漏洞绕过安全机制执行未授权操作，导致缓冲区溢出，执行远程代码，造成拒绝服务。此外，CloudBees、Google、Moxa 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，执行任意代码，造成拒绝服务（无限循环）等。Sony BRAVIA Smart TVs 被披露存在拒绝服务漏洞。

攻击者可利用该漏洞造成电视卡屏，无法响应，程序崩溃并且导致电视重启。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、Invoxia NVX220 信任管理问题漏洞

验证描述

Invoxia NVX220 是法国 Invoxia 公司的一款 IP 电话机。

Invoxia NVX220 中存在信任管理问题漏洞。攻击者可利用该漏洞访问自定义的 CLI。

验证信息

POC 链接：https://gitlab.com/r3dlight/CVE-2018-14528

参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2019-23976

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. Palo Alto Networks VPN 漏洞曝光，允许黑客远程执行任意代码

据外媒报道，研究人员发现 Palo Alto Networks 的 GlobalProtect 产品存在一个关键的 RCE 漏洞，允许黑客利用该漏洞向易受攻击的 SSL VPN 目标发送特制请求，远程执行系统上的代码。

参考链接：https://zhuanlan.zhihu.com/p/74841727

2. Comodo Antivirus 受到多个漏洞的影响

专家们发现了 Comodo Antivirus 中的一些漏洞，其中最严重的漏洞 CVE-2019-3969，可被攻击者利用，访问目标系统以逃离 Comodo Antivirus 沙箱并将提升系统权限。

参考链接：https://securityaffairs.co/wordpress/88800/hacking/comodo-antivirus-flaws.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