国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2019 年 08 月 19 日-2019 年 08 月 25 日 **2019 年第 34 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 383 个，其中高危漏洞 104 个、中危漏洞 264 个、低危漏洞 15 个。漏洞平均分值为 5.93。本周收录的漏洞中，涉及 0day 漏洞 89 个（占 23%），其中互联网上出现“Bento4 越界读取漏洞、Bento4 空指针解引用漏洞（CNVD-2019-28477）”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 1865 个，与上周（1469 个）环比增长 27%。

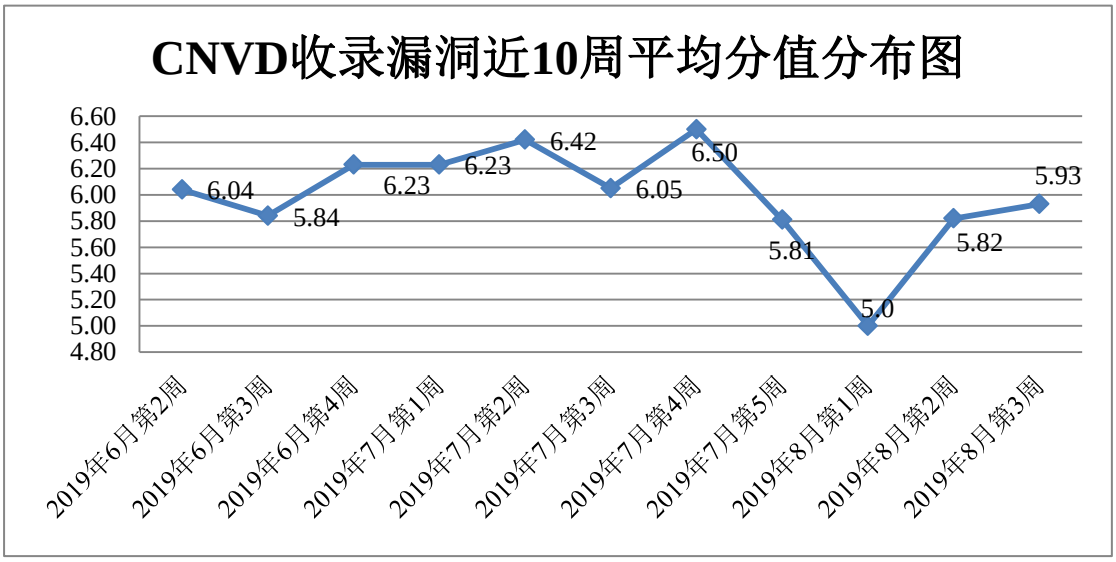

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 7 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 265 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 52 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18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：

四川挚梦科技有限公司、中国储备粮管理集团有限公司、摩莎科技（上海）有限公司、珠海创新网络科技有限公司、淄博闪灵网络科技有限公司、盘古网络科技有限公司、山西先启科技有限公司、上海丹帆网络科技有限公司、航天工业发展股份有限公司、苏州恩斯特网络科技有限公司、铭飞科技有限公司、北京天地华大网络技术有限公司、大庆紫金桥软件技术有限公司、江苏泰得科技股份有限公司、合肥柒帮网络科技有限公司、三菱电机自动化（中国）有限公司、上海财联社金融科技有限公司、上海若美网络科技有限公司、西安欧必信息技术有限公司、北京光影娱乐科技有限公司、暇光软件科技（上海）有限公司、上海财联社金融科技有限公司、上海若美网络科技有限公司、西安欧必信息技术有限公司、北京光影娱乐科技有限公司、暇光软件科技（上海）有限公司、成都鹏博士电信传媒集团股份有限公司、ABB 集团、中国橡胶工业协会乳胶分会、中国电器工业协会防爆电器分会、中国科技开发院、中国工控网、中国行业研究网、宜兰网页设计中心、米酷影视、海洋 CMS、ZZCMS 和 ShopXO。

本周，CNVD 发布了《关于高通 WLAN 芯片存在远程代码执行漏洞的安全公告》。详情参见 CNVD 网站公告内容。

https://www.cnvd.org.cn/webinfo/show/5175

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、北京神州绿盟科技有限公司、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。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、北京铭图天成信息技术有限公司、国瑞数码零点实验室、山东华鲁科技发展股份有限公司、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、上海银基信息安全技术股份有限公司、国网思极检测技术（北京）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、浙江国利网安科技有限公司、广州非凡信息安全技术有限公司、远江盛邦（北京）网络安全科技股份有限公司、北京智游网安科技有限公司、贵州安码科技有限公司、广州锦行网络科技有限公司、山东九州信泰信息科技股份有限公司、山石网科通信技术有限公司、上海市信息安全测评认证中心及其他个人白帽子向 CNVD 提交了 1865 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 1332 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
奇安信网神（补天平台）	776	776
斗象科技（漏洞盒子）	556	556
北京天融信网络安全技术有限公司	388	4
哈尔滨安天科技集团股份有限公司	231	0
北京神州绿盟科技有限公司	207	3
深信服科技股份有限公司	91	0
新华三技术有限公司	83	0
厦门服云信息科技有限公司	71	0
华为技术有限公司	66	0
北京启明星辰信息安全技术有限公司	51	0
北京数字观星科技有限公司	23	0
西安四叶草信息技术有限公司	13	13
中新网络信息安全股份有限公司	13	13
四川无声信息技术有限公司	12	12
南京联成科技发展股份有限公司	2	2
北京知道创宇信息技术股份有限公司	1	0
南京众智维信息科技有限公司	94	94
山东云天安全技术有限公司	52	52
北京铭图天成信息技术有限公司	39	39
国瑞数码零点实验室	32	32
山东华鲁科技发展股份有限公司	25	25

任子行网络技术股份有限公司	20	20
长春嘉诚信息技术股份有限公司	17	17
上海银基信息安全技术股份有限公司	10	10
国网思极检测技术（北京）有限公司	6	6
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	5	5
浙江国利网安科技有限公司	3	3
广州非凡信息安全技术有限公司	3	3
远江盛邦（北京）网络安全科技股份有限公司	3	3
内蒙古奥创科技有限公司	3	3
北京智游网安科技有限公司	2	2
贵州安码科技有限公司	2	2
广州锦行网络科技有限公司	1	1
山东九州信泰信息科技股份有限公司	1	1
山石网科通信技术有限公司	1	1
上海市信息安全测评认证中心	1	1
CNCERT 宁夏分中心	10	10
CNCERT 天津分中心	5	5
CNCERT 贵州分中心	1	1
CNCERT 四川分中心	1	1
CNCERT 西藏分中心	1	1
个人	142	142

报送总计	3070	1865

本周漏洞按类型和厂商统计

本周，CNVD 收录了 383 个漏洞。应用程序 307 个，操作系统 34 个，WEB 应用 23 个，网络设备（交换机、路由器等网络端设备）10 个，智能设备（物联网终端设备）6 个，安全产品 3 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	307
操作系统	34
WEB 应用	23
网络设备（交换机、路由器等网络端设备）	10
智能设备（物联网终端设备）	6
安全产品	3

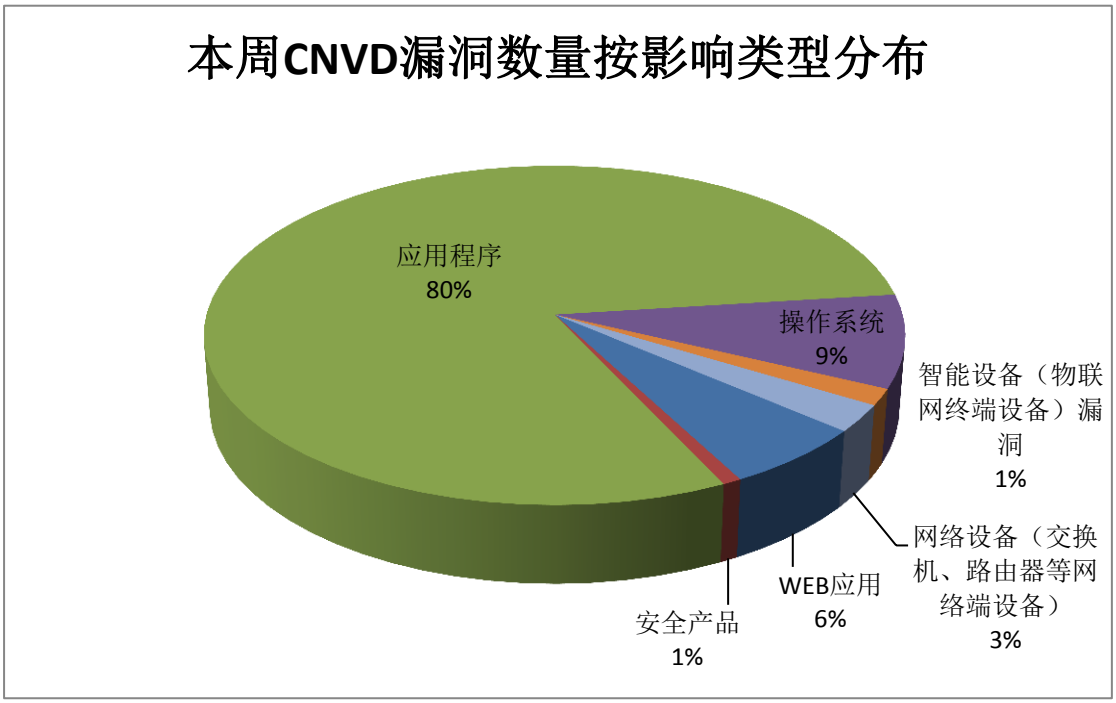

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Oracle、Adobe、Google 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	Oracle	133	35%
2	Adobe	43	11%
3	Google	24	6%
4	NVIDIA	19	5%
5	CloudBees	18	5%
6	Bento4	14	4%
7	MATIO	13	3%
8	HP	12	3%
9	OpenSC	11	3%
10	其他	96	25%

本周行业漏洞收录情况

本周，CNVD 收录了 1 个电信行业漏洞，23 个移动互联网行业漏洞，6 个工控行业漏洞（如下图所示）。其中，“Google Android System 存在未明漏洞、LCDS LAquis SCADA 存在未明漏洞”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/

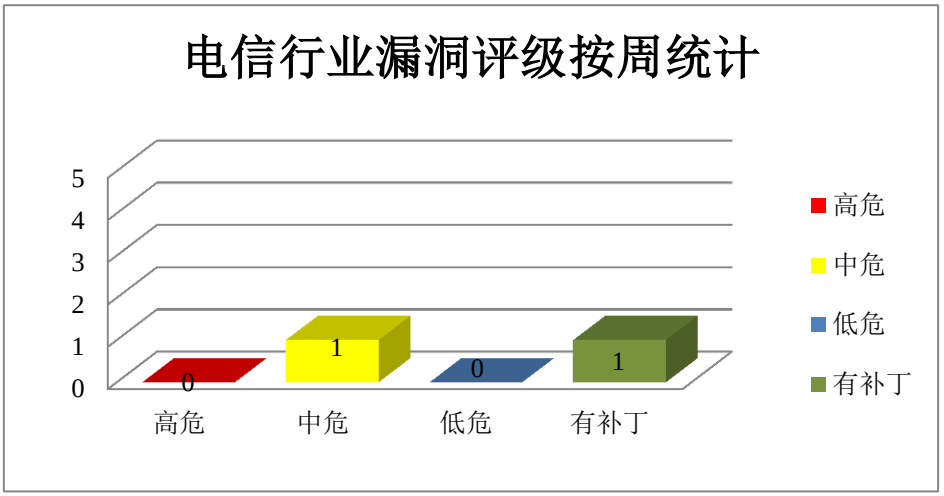

图 3 电信行业漏洞统计

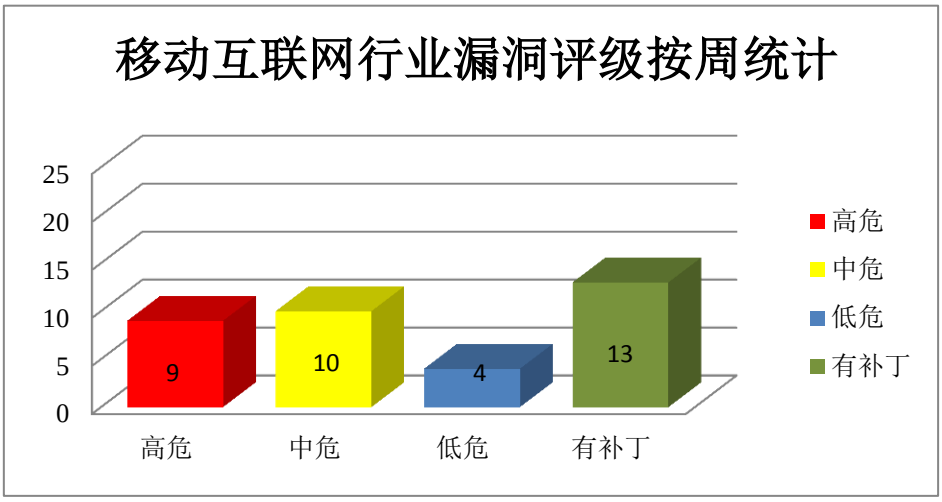

图 4 移动互联网行业漏洞统计

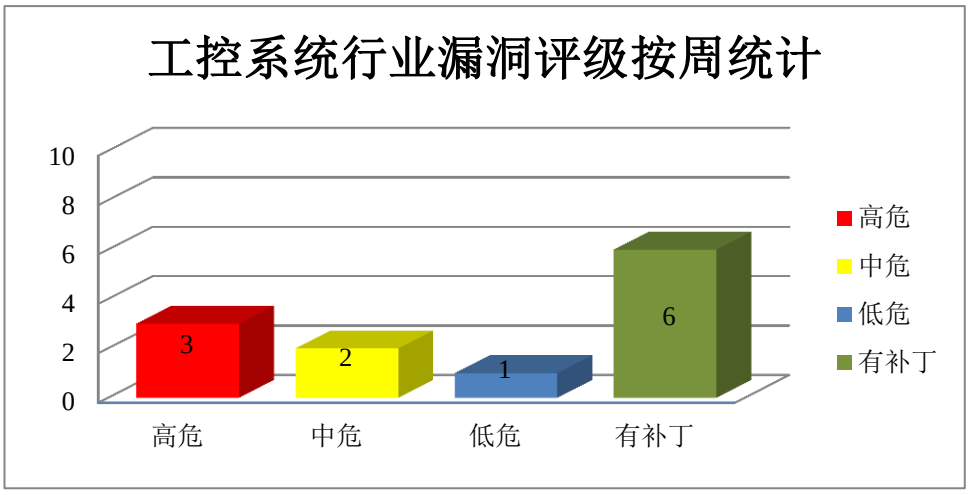

图 5 工控系统行业漏洞统计

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、 Qualcomm WLAN 芯片远程代码执行漏洞

Qualcomm WLAN 芯片是高通平台处理 WLAN/WIFI 协议的专用芯片，属于高通 Baseband 子系统，用于提高 WLAN/WIFI 处理速度和性能，降低能耗。本周，该产品被披露存在远程代码执行漏洞，攻击者可以通过控制 WLAN 固件，最终导致在服务器上执行任意代码。

CNVD 收录的相关漏洞包括：ualcomm WLAN 芯片远程代码执行漏洞。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-2019-28290

2、Oracle 产品安全漏洞

Oracle Fusion Middleware（Oracle 融合中间件）是一套面向企业和云环境的业务创新平台。该平台提供了中间件、软件集合等功能。Outside In Technology 是其中的一个软件开发工具包组件。本周，上述产品被披露存在访问控制错误漏洞，攻击者可利用漏洞未授权读取数据，造成拒绝服务，影响数据的保密性和可用性。。

CNVD 收录的相关漏洞包括：Oracle Outside In Technology 访问控制错误漏洞（CNVD-2019-27776、CNVD-2019-27777、CNVD-2019-27778、CNVD-2019-27779、CNVD-2019-27780、CNVD-2019-27781、CNVD-2019-27783、CNVD-2019-27784）。其中，“Oracle Outside In Technology 访问控制错误漏洞（CNVD-2019-27784）”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-2019-27776
http://www.cnvd.org.cn/flaw/show/CNVD-2019-27777
http://www.cnvd.org.cn/flaw/show/CNVD-2019-27778
http://www.cnvd.org.cn/flaw/show/CNVD-2019-27779
http://www.cnvd.org.cn/flaw/show/CNVD-2019-27780
http://www.cnvd.org.cn/flaw/show/CNVD-2019-27781
http://www.cnvd.org.cn/flaw/show/CNVD-2019-27783
http://www.cnvd.org.cn/flaw/show/CNVD-2019-27784

3、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，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-2019-28672、CNVD-2019-28686、CNVD-2019-28688、、CNVD-2019-28689、CNVD-2019-28690、CNVD-2019-28691、CNVD-2019-28692、CNVD-2019-28693）。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-2019-28672
http://www.cnvd.org.cn/flaw/show/CNVD-2019-28686
http://www.cnvd.org.cn/flaw/show/CNVD-2019-28688
http://www.cnvd.org.cn/flaw/show/CNVD-2019-28689
http://www.cnvd.org.cn/flaw/show/CNVD-2019-28690
http://www.cnvd.org.cn/flaw/show/CNVD-2019-28691
http://www.cnvd.org.cn/flaw/show/CNVD-2019-28692

http://www.cnvd.org.cn/flaw/show/CNVD-2019-28693

4、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多个漏洞，攻击者可利用漏洞获取敏感信息，执行代码，造成拒绝服务。

CNVD 收录的相关漏洞包括：Google Android WLAN 整数溢出漏洞、Google Android WLAN 空指针逆向引用漏洞、Google Android WLAN 缓冲区溢出漏洞（CNVD-2019-28607、CNVD-2019-28611）、Google Android WLAN 双重释放漏洞、Google Android System 信息泄露漏洞（CNVD-2019-28627、CNVD-2019-28634）、Google Android Media Framework 远程代码执行漏洞（CNVD-2019-28638）。其中，除“Google Android System 信息泄露漏洞（CNVD-2019-28627、CNVD-2019-28634）”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-2019-28606

http://www.cnvd.org.cn/flaw/show/CNVD-2019-28604

http://www.cnvd.org.cn/flaw/show/CNVD-2019-28607

http://www.cnvd.org.cn/flaw/show/CNVD-2019-28611

http://www.cnvd.org.cn/flaw/show/CNVD-2019-28615

http://www.cnvd.org.cn/flaw/show/CNVD-2019-28627

http://www.cnvd.org.cn/flaw/show/CNVD-2019-28634

http://www.cnvd.org.cn/flaw/show/CNVD-2019-28638

5、NVIDIA 产品安全漏洞

NVIDIA Windows GPU Display Driver 是一款专用于 Windows 平台的图形处理器（GPU）显卡驱动程序。NVIDIA SHIELD TV 娱乐主机是一款客厅娱乐设备。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞执行代码，提升权限，泄露信息或造成拒绝服务。

CNVD 收录的相关漏洞包括：NVIDIA Windows GPU Display Driver 权限许可和访问控制问题漏洞（CNVD-2019-28285、CNVD-2019-28287）、NVIDIA Windows GPU Display Driver 输入验证错误漏洞、NVIDIA Windows GPU Display Driver 代码问题漏洞、NVIDIA Shield TV Experience 权限许可和访问控制漏洞、NVIDIA Windows GPU Display Driver 拒绝服务漏洞（CNVD-2019-28599、CNVD-2019-28600、CNVD-2019-28601）。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-2019-28285

http://www.cnvd.org.cn/flaw/show/CNVD-2019-28286

http://www.cnvd.org.cn/flaw/show/CNVD-2019-28287

http://www.cnvd.org.cn/flaw/show/CNVD-2019-28483

http://www.cnvd.org.cn/flaw/show/CNVD-2019-28488

http://www.cnvd.org.cn/flaw/show/CNVD-2019-28599

http://www.cnvd.org.cn/flaw/show/CNVD-2019-28600

http://www.cnvd.org.cn/flaw/show/CNVD-2019-28601

6、CloudBees Jenkins Wall Display Plugin 跨站脚本漏洞

CloudBees Jenkins（Hudson Labs）是一套基于 Java 开发的持续集成工具。本周，CloudBees Jenkins Wall Display Plugin 被披露存在跨站脚本漏洞。攻击者可利用该漏洞执行客户端代码。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-2019-28234

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-2019-28115	HPE 3PAR StoreServ Management Console 授权绕过漏洞（CNVD-2019-28115）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://h20392.www2.hpe.com/portal/swdepot/displayProductInfo.do?productNumber=SSMC_CONSOLE
CNVD-2019-28653	Adobe Photoshop CC 堆溢出漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://helpx.adobe.com/security/products/photoshop/apsb19-44.html
CNVD-2019-28119	HPE 3PAR Service Processor 安全限制绕过漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbst03942en_us
CNVD-2019-28640	Microsoft Edge Chakra 脚本引擎内存破坏漏洞（CNVD-2019-28640）	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-2019-1140
CNVD-2019-28279	Philips e-Alert 输入验证漏洞	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.usa.philips.com/healthcare/about/customer-support/product-security

CNVD-2019-28426	Oracle Solaris 存在未明漏洞（CNVD-2019-28426）	高	厂商已发布漏洞修复程序，请及时关注更新：https://www.oracle.com/technetwork/security-advisory/cpujan2019-5072801.html
CNVD-2019-28639	Microsoft Edge Chakra 脚本引擎内存破坏漏洞（CNVD-2019-28639）	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-2019-1197
CNVD-2019-28117	HPE 3PAR Service Processor 越权访问漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbst03942en_us
CNVD-2019-28652	Adobe Acrobat/Reader 堆溢出漏洞（CNVD-2019-28652）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://helpx.adobe.com/security/products/acrobat/apsb19-41.html
CNVD-2019-28120	HPE 3PAR Service Processor 认证绕过漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbst03942en_us

小结：本周，Qualcomm WLAN 芯片被披露存在远程代码执行漏洞，攻击者可以通过控制 WLAN 固件，最终导致在服务器上执行任意代码。此外，Oracle、Adobe、Google 等多款产品被披露存在多个漏洞，攻击者可利用漏洞执行代码，提升权限，泄露信息或造成拒绝服务等。另外，CloudBees Jenkins Wall Display Plugin 被披露存在跨站脚本漏洞，攻击者可利用该漏洞执行客户端代码。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、Bento4 越界读取漏洞

验证描述

Bento4 是一款用于读写 MP4 文件的开源的 C++库。

Bento4 1.5.1-628 版本中存在越界读取漏洞。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。

验证信息

POC 链接：https://research.loginsoft.com/vulnerability/a-heap-buffer-overflow-vulnerability-in-the-function-ap4_bitstreamreadbytes-bento4-1-5-1-628/

参考链接：http://www.cnvd.org.cn/flaw/show/CNVD-2019-28472

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. Facebook 新的设计中的安全漏洞允许攻击者从用户的个人资料中删除任何照片

某安全专家早期获得了 Facebook 对新 FB5 设计的访问权，并发现了一个重要的设计缺陷。Harewood 解释说，这个问题会影响 GraphQL，这是在新设计中实现的一个功能，用于从 Facebook 粉丝页面删除个人资料图片。因此，攻击者可能会滥用设计漏洞从用户配置文件中删除照片。

参考链接：https://securityaffairs.co/wordpress/90136/social-networks/facebook-fb5-design-flaw.html

2. 澳大利亚 Cuscal 赞助的一家金融机构出现漏洞，导致 PayID 信息泄露

澳大利亚新支付平台（NPP）的 PayID 查找功能再一次成为网络攻击的目标，这次地址服务中的一些记录和相关数据被泄露。NPP 澳大利亚公司（负责监督通过该系统进行的所有交易的公司）周二证实，该数据暴露是 Cuscal Limited 赞助的一家金融机构中的漏洞所导致。

参考链接：https://www.zdnet.com/article/payids-exposed-at-the-hands-of-aussie-cuscal-sponsored-financial-institution/

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