国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2019 年 12 月 23 日-2019 年 12 月 29 日 **2019 年第 52 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 203 个，其中高危漏洞 67 个、中危漏洞 118 个、低危漏洞 18 个。漏洞平均分值为 5.83。本周收录的漏洞中，涉及 0day 漏洞 93 个（占 46%），其中互联网上出现“libIEC61850 'BerDecoder_decodeUint32'函数缓冲区溢出漏洞、RIOT RIOT-OS 拒绝服务漏洞”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 3493 个，与上周（3156 个）环比增长 10%。

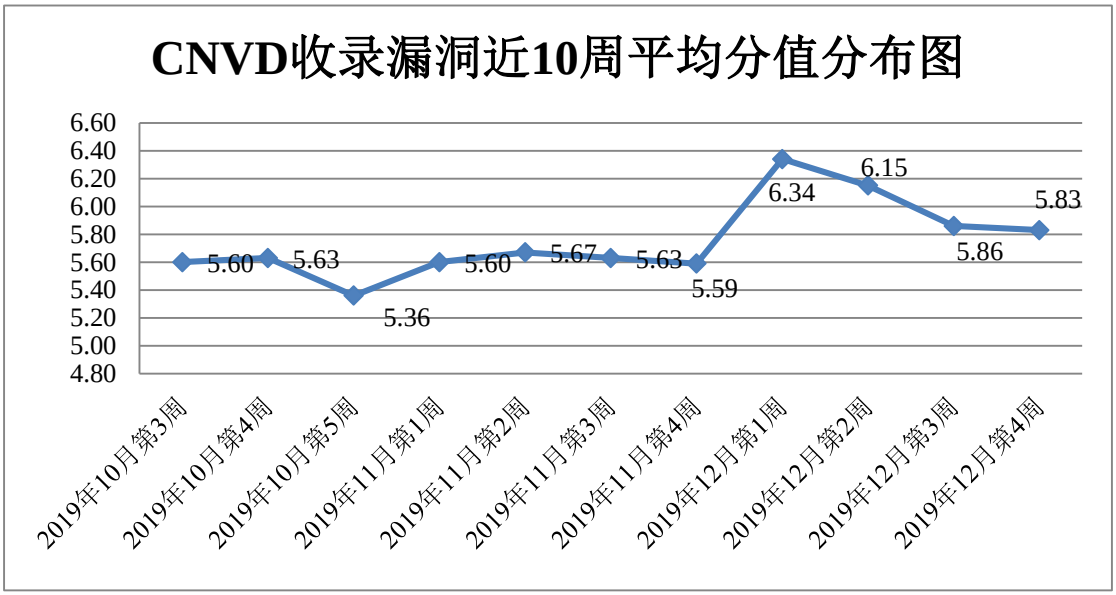

图 1 CNVD 收录漏洞近 10 周平均分值分布图

本周漏洞事件处置情况

本周，CNVD 向银行、保险、能源等重要行业单位通报漏洞事件 13 起，向基础电信企业通报漏洞事件 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 343 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 48 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 7 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：

杭州览坤科技有限公司、成都鹏博士电信传媒集团股份有限公司、郑州锐马科技有限公司、沧州市凡诺广告传媒有限公司、太原天祥科技有限公司、揭阳市集科计算机网络有限公司、深圳迪元素科技有限公司、深圳市威纶通科技有限公司、geoserver 公司、金蝶软件有限公司、上海泛微网络科技股份有限公司、飞友科技有限公司、北京亿中邮信息技术有限公司、上海立仓网络科技有限公司、上海商创网络科技有限公司、中铁上海设计院徐州分公司、中铁上海工程局集团第一工程有限公司、中铁上海工程局集团有限公司、北京用友政务软件股份有限公司、北京良精志诚科技有限责任公司、深圳锟铻科技有限公司、杭州乐邦科技有限公司、青岛灼灼文化传媒有限公司、洛阳云业信息科技有限公司、美图公司、上海翼浩信息科技有限公司、湖南壹拾捌号网络技术有限公司、拓尔思信息技术股份有限公司、上海二三四五网络科技有限公司、深圳市迪元素科技有限公司、广州网际快车电子有限公司、南京奋斗网络科技有限公司、西安佰联网络技术有限公司、普联技术有限公司、东莞市一鸣网络科技公司、呼和浩特市网域科技有限责任公司、山西众众行网络科技有限公司、安庆怀宁县君成网络科技有限公司、福州网钛软件科技有限公司、网际傲游(北京)科技有限公司、中铁上海局、小米科技有限责任公司、北京魔方恒久软件有限公司、长沙德尚网络科技有限公司、昆明云涛科技有限公司、淄博闪灵网络科技有限公司、厦门凤凰创壹软件有限公司、浙大恩特网络科技有限公司、太原飞扬动力科技有限公司、杭州欢创科技有限公司、昆山联众网络科技有限公司、海南赞赞网络科技有限公司、北京世纪超星信息技术发展有限责任公司、摩莎科技（上海）有限公司、睿谷信息科技有限公司、中国建材集团有限公司、广州万户网络技术有限公司、茉柏枘（上海）软件科技有限公司、海盐创宜软件科技有限公司、靖江市新超云网络技术服务有限公司、北京旷视科技有限公司、广州齐博网络科技有限公司、全讯汇聚网络科技（北京）有限公司、上海银狐信息科技有限公司、北京椒图科技有限公司、国家卫生健康委人才交流服务中心、中国人才研究会金融人才专业委员会、华科网络、Oracle、海洋 CMS、WDJA、发货 100、miniCMS、zzzcms 和 ZKEASOFT。

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、中新网络信息安全股份有限公司、华为技术有限公司、北京神州绿盟科技有限公司等单位报送公开收集的漏洞数量较多。内蒙古奥创科技有限公司、远江盛邦（北京）网络安全科技股份有限公司、内蒙古洞明科技有限公司、河南灵创电

子科技有限公司 、北京华云安信息技术有限公司、北京铭图天成信息技术有限公司、北京网思科平科技有限公司、山东新潮信息技术有限公司、杭州迪普科技股份有限公司、河南信安世纪科技有限公司、杭州海康威视数字技术股份有限公司、山东云天安全技术有限公司、国瑞数码零点实验室、上海端御信息科技有限公司、广州美杜莎网络科技有限公司、中移（杭州）信息技术有限公司、京东云安全、北京智游网安科技有限公司、山东华鲁科技发展股份有限公司及其他个人白帽子向 CNVD 提交了 3493 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）、斗象科技（漏洞盒子）和上海交大向 CNVD 共享的白帽子报送的 2682 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）	1097	1097
上海交大	865	865
奇安信网神（补天平台）	720	720
北京天融信网络安全技术有限公司	326	2
哈尔滨安天科技集团股份有限公司	195	0
中新网络信息安全股份有限公司	135	135
华为技术有限公司	108	0
北京神州绿盟科技有限公司	107	4
深信服科技股份有限公司	61	0
新华三技术有限公司	55	0
北京启明星辰信息安全技术有限公司	46	0
恒安嘉新(北京)科技股份公司	42	0
厦门服云信息科技有限公司	38	0
西安四叶草信息技术有限公司	32	32
中国电信集团系统集成有限责任公司	30	30
北京数字观星科技有限公司	19	0

四川无声信息技术有限公司	7	7
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
内蒙古奥创科技有限公司	64	64
远江盛邦（北京）网络安全科技股份有限公司	62	62
内蒙古洞明科技有限公司	45	45
河南灵创电子科技有限公司	35	35
北京华云安信息技术有限公司	21	21
北京铭图天成信息技术有限公司	20	20
北京网思科平科技有限公司	14	14
山东新潮信息技术有限公司	14	14
杭州迪普科技股份有限公司	14	0
河南信安世纪科技有限公司	11	11
杭州海康威视数字技术股份有限公司	10	10
山东云天安全技术有限公司	5	5
国瑞数码零点实验室	3	3
上海端御信息科技有限公司	3	3
广州美杜莎网络科技有限公司	2	2
中移（杭州）信息技术有限公司	1	1
京东云安全	1	1
北京智游网安科技有限公司	1	1
山东华鲁科技发展股份有限公司	1	1

CNCERT 河北分中心	17	17
CNCERT 甘肃分中心	8	8
CNCERT 贵州分中心	3	3
CNCERT 吉林分中心	1	1
个人	258	258
报送总计	4500	3493

本周漏洞按类型和厂商统计

本周，CNVD 收录了 203 个漏洞。应用程序 76 个，操作系统 50 个，WEB 应用 45 个，网络设备（交换机、路由器等网络端设备）24 个，安全产品 4 个，智能设备（物联网终端设备）4 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	76
操作系统	50
WEB 应用	45
网络设备（交换机、路由器等网络端设备）	24
安全产品	4
智能设备（物联网终端设备）漏洞	4

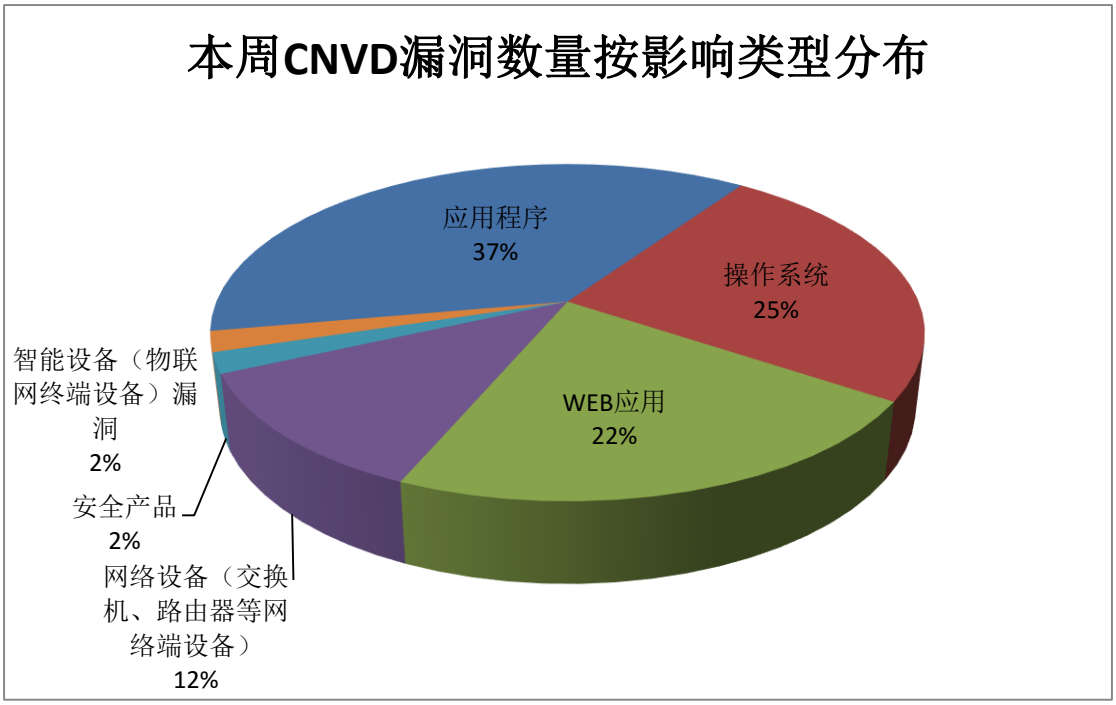

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 linux、Google、Apple 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	linux	23	11%
2	Google	23	11%
3	Apple	16	8%
4	IBM	13	7%
5	中兴通讯股份有限公司 ZTE	10	6%
6	Huawei	6	3%
7	Barco	5	2%
8	湖南考试在线网络科技有限公司	5	2%
9	SAP	4	2%
10	其他	98	48%

本周行业漏洞收录情况

本周，CNVD 收录了 13 个电信行业漏洞，28 个移动互联网行业漏洞，5 个工控行业漏洞（如下图所示）。其中，“Google Android 操作系统命令注入漏洞、D-Link DIR-615 授权问题漏洞、Google Android 缓冲区溢出漏洞（CNVD-2019-47020）、Google Android Kernel 权限提升漏洞（CNVD-2019-47018）”的综合评级为“高危”。相关厂商已经发布了漏洞的修补程序，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/

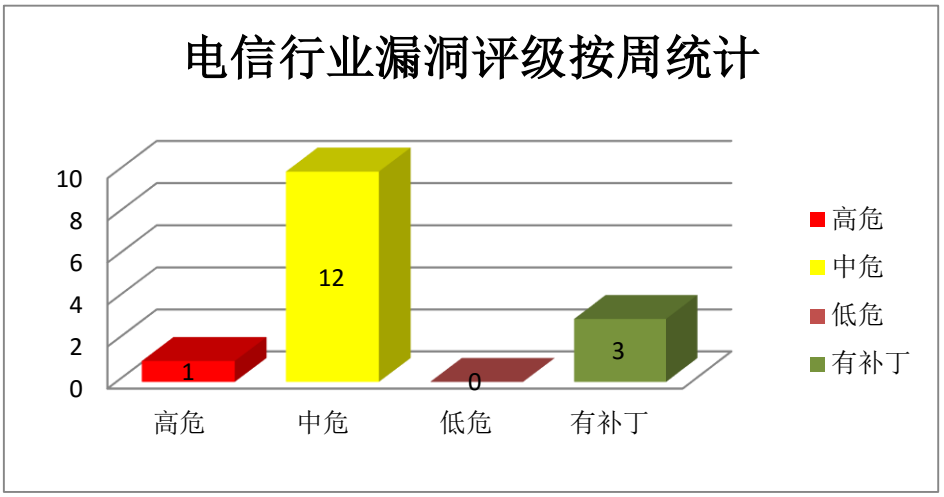

图 3 电信行业漏洞统计

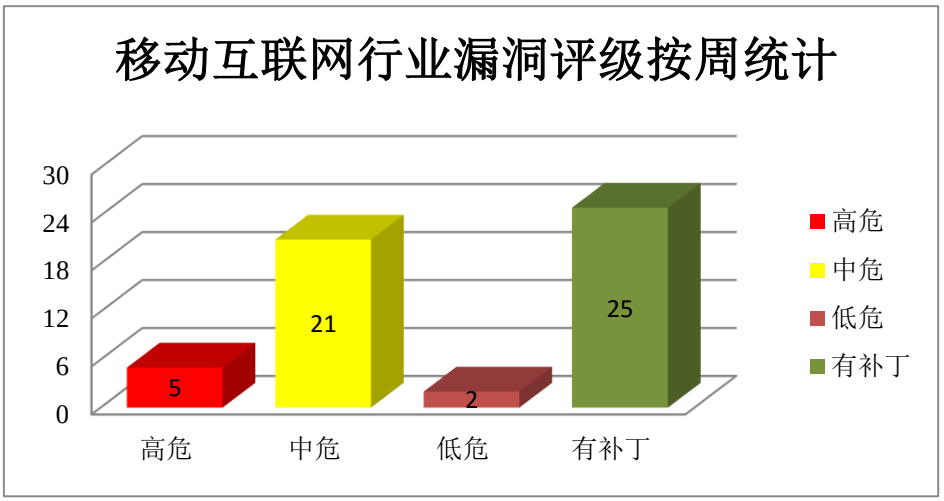

图 4 移动互联网行业漏洞统计

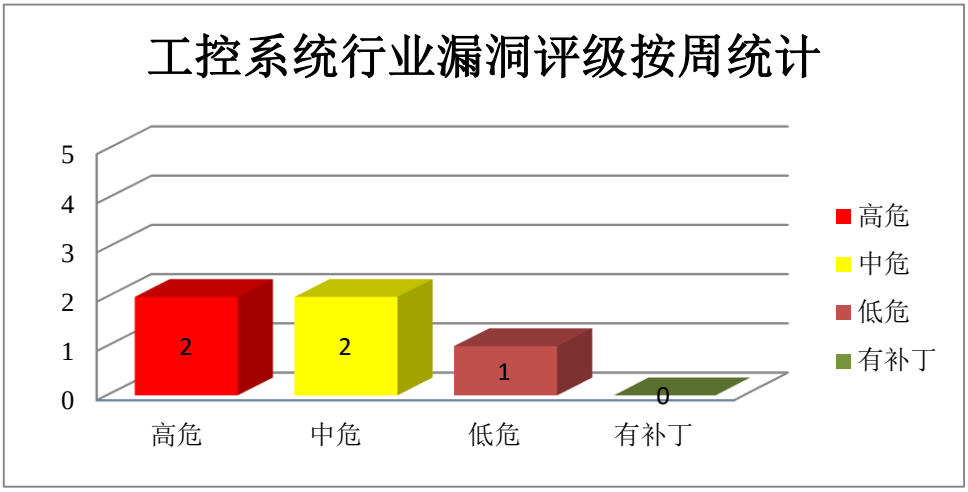

图 5 工控系统行业漏洞统计

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、Linux 产品安全漏洞

Linux kernel 是美国 Linux 基金会发布的开源操作系统 Linux 所使用的内核。Marvell WiFi chip driver 是其中的的一个 WiFi 芯片驱动程序。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞导致缓冲区溢出，造成内核异常。

CNVD 收录的相关漏洞包括：Linux kernel 内存错误引用漏洞（CNVD-2019-46994、CNVD-2019-47002）、Linux kernel 缓冲区溢出漏洞（CNVD-2019-46998、CNVD-2019-47005）、Linux kernel 输入验证错误漏洞（CNVD-2019-47001）、Linux Kernel 堆缓冲区溢出漏洞（CNVD-2019-47003）、Linux kernel Marvell WiFi chip driver 缓冲区溢出漏洞、Linux Kernel 'marvell/mwifiex/scan.c'文件缓冲区溢出漏洞。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-2019-46994

http://www.cnvd.org.cn/flaw/show/CNVD-2019-46999

http://www.cnvd.org.cn/flaw/show/CNVD-2019-46998

http://www.cnvd.org.cn/flaw/show/CNVD-2019-47001

http://www.cnvd.org.cn/flaw/show/CNVD-2019-47003

http://www.cnvd.org.cn/flaw/show/CNVD-2019-47002

http://www.cnvd.org.cn/flaw/show/CNVD-2019-47007

http://www.cnvd.org.cn/flaw/show/CNVD-2019-47005

2、Google 产品安全漏洞

Google Chrome 是美国谷歌（Google）公司的一款 Web 浏览器。Android 是美国谷歌（Google）和开放手持设备联盟（简称 OHA）的一套以 Linux 为基础的开源操作系统。Video driver 是其中的一个视频驱动程序。MNH driver 是其中的一个 MNH 驱动程序。Broadcom Bluetooth 是其中的一个蓝牙组件。Kernel 是其中的一个系统内核组件。Touch driver 是其中的一个触控驱动程序。Framework 是其中的一个 Android 框架组件。LG Bootloader 是其中的一个启动加载程序。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞提升权限，执行任意代码，导致拒绝服务。

CNVD 收录的相关漏洞包括：Google Chrome 资源管理错误漏洞（CNVD-2019-46750）、Google Android Video 驱动程序提权漏洞、Google Android MNH 驱动程序权限提升漏洞、Google Android Broadcom Bluetooth 权限提升漏洞、Google Android Kernel 权限提升漏洞（CNVD-2019-47018）、Google Android Touch 驱动程序权限提升漏洞、Google Android 缓冲区溢出漏洞（CNVD-2019-47020）、Google Android 操作系统命令注入漏洞。其中，“Google Chrome 资源管理错误漏洞（CNVD-2019-46750）、Google Android Kernel 权限提升漏洞（CNVD-2019-47018）、Google Android 缓冲区溢出漏洞（CNVD-2019-47020）、Google Android 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-2019-46750

http://www.cnvd.org.cn/flaw/show/CNVD-2019-47015

http://www.cnvd.org.cn/flaw/show/CNVD-2019-47016

http://www.cnvd.org.cn/flaw/show/CNVD-2019-47017

http://www.cnvd.org.cn/flaw/show/CNVD-2019-47018

http://www.cnvd.org.cn/flaw/show/CNVD-2019-47019

http://www.cnvd.org.cn/flaw/show/CNVD-2019-47020

http://www.cnvd.org.cn/flaw/show/CNVD-2019-47021

3、Apple 产品安全漏洞

Apple Safari 等都是美国苹果（Apple）公司的产品。Apple Safari 是一款 Web 浏览器，是 Mac OS X 和 iOS 操作系统附带的默认浏览器。Apple iOS 是一套为移动设备所开发的操作系统。Apple watchOS 是一套智能手表操作系统。WebKit 是其中的一个 Web 浏览器引擎组件。Apple iCloud for Windows 是一款基于 Windows 平台的云服务。CoreCrypto 是其中的一个核心加密组件。Apple macOS Catalina 是一套专为 Mac 计算机所开发的专用操作系统。libxslt 是其中的一个 XSLT（可扩展样式表转换语言）库。CFNetwork 是其中的一个低层次、高性能的框架，是 BSD sockets（套接字）的扩展。Apple tvOS 是一套智能电视操作系统。Kernel 是其中的一个内核组件。Apple iTunes for Windows 是一款基于 Windows 平台的媒体播放器应用程序。WebKit 是其中的一个 Web 浏览器引擎组件。Apple iPadOS 是一套用于 iPad 平板电脑的操作系统。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞执行任意代码，导致拒绝服务等。

CNVD 收录的相关漏洞包括：多款 Apple 产品 WebKit 组件内存破坏漏洞（CNVD-2019-46956、CNVD-2019-46969）、多款 Apple 产品 WebKit 组件代码执行漏洞（CNVD-2019-46964）、多款 Apple 产品 libxslt 组件内存破坏漏洞、多款 Apple 产品 Kernel 组件内存破坏漏洞（CNVD-2019-46965）、多款 Apple 产品 CFNetwork 组件跨站脚本漏洞、多款 Apple 产品 CoreCrypto 组件拒绝服务漏洞、多款 Apple 产品 Kernel 组件代码执行漏洞（CNVD-2019-46966）。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-2019-46956

http://www.cnvd.org.cn/flaw/show/CNVD-2019-46958

http://www.cnvd.org.cn/flaw/show/CNVD-2019-46965

http://www.cnvd.org.cn/flaw/show/CNVD-2019-46964

http://www.cnvd.org.cn/flaw/show/CNVD-2019-46963

http://www.cnvd.org.cn/flaw/show/CNVD-2019-46969

http://www.cnvd.org.cn/flaw/show/CNVD-2019-46967

http://www.cnvd.org.cn/flaw/show/CNVD-2019-46966

4、IBM 产品安全漏洞

IBM Spectrum Scale 是美国 IBM 公司的一套基于 IBM GPFS（专为 PB 级存储管理而优化的企业文件管理系统）的可扩展的数据及文件管理解决方案。IBM Financial Transaction Manager for SWIFT Services 是美国 IBM 公司的一款金融事务管理器产品。IBM Cognos Analytics 是美国 IBM 公司的一套商业智能软件。IBM Planning Analytics 是美国 IBM 公司的一套业务规划分析解决方案。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 cookie 值，执行任意命令等。

CNVD 收录的相关漏洞包括：IBM Spectrum Scale 输入验证错误漏洞、IBM Financial Transaction Manager for SWIFT Services 点击劫持漏洞、IBM Financial Transaction Manager for SWIFT Services 跨站脚本漏洞、IBM Financial Transaction Manager for SWIFT Services 信息泄露漏洞、IBM Financial Transaction Manager for SWIFT Services 跨站请求伪造漏洞、IBM Cognos Analytics 跨站脚本漏洞（CNVD-2019-46620）、IBM Cognos Analytics 跨站请求伪造漏洞、IBM Planning Analytics 代码执行漏洞。其中，“IBM Spectrum Scale 输入验证错误漏洞、IBM Planning Analytics 代码执行漏洞”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-2019-46449

http://www.cnvd.org.cn/flaw/show/CNVD-2019-46616

http://www.cnvd.org.cn/flaw/show/CNVD-2019-46617

http://www.cnvd.org.cn/flaw/show/CNVD-2019-46618

http://www.cnvd.org.cn/flaw/show/CNVD-2019-46619

http://www.cnvd.org.cn/flaw/show/CNVD-2019-46620

http://www.cnvd.org.cn/flaw/show/CNVD-2019-46621

http://www.cnvd.org.cn/flaw/show/CNVD-2019-46977

5、Linux kernel 内存错误引用漏洞（CNVD-2019-46996）

Linux kernel 是一种计算机操作系统内核。本周，Linux kernel 被披露存在内存错误引用漏洞。攻击者可利用该漏洞导致发生释放后重用。目前，厂商尚未发布上述漏洞的修补程序。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-2019-46996

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-2019-46444	Barco ClickShare Button R9861500D01 凭据保护不足漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.barco.com
CNVD-2019-46640	Newbee-mall 存在 SQL 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://github.com/newbee-ltd/newbee-mall
CNVD-2019-46983	D-Link DIR-615 授权问题漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：http://www.dlink.com/
CNVD-2019-46985	Embedthis Software GoAhead 资源管理错误漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.embedthis.com
CNVD-2019-46986	SiteVision 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.sitevision.se
CNVD-2019-46446	Barco ClickShare Button R9861500D01 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://www.barco.com
CNVD-2019-47013	Linux kernel KVM hypervisor 内存错误引用漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.linux-kvm.org/page/Main_Page
CNVD-2019-47027	TYPO3 SQL 注入漏洞（CNVD-2019-47027）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://typo3.org/security/advisory/typo3-core-sa-2011-002/
CNVD-2019-47196	GraphicsMagick magick/error.c 文件资源管理错误漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：http://hg.graphicsmagick.org/hg/GraphicsMagick/rev/44ab7f6c20b4
CNVD-2019-47200	Open TFTP Server MT 'logMess'函数缓冲区溢出漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://sourceforge.net/p/tftp-server/discussion/550564/thread/a586ce62/

小结：本周，Linux 产品被披露存在多个漏洞，攻击者可利用漏洞导致缓冲区溢出，造成内核异常。此外，Google、Apple、IBM 等多款产品被披露存在多个漏洞，攻击者可利用漏洞获取 cookie 值，提升权限，执行任意代码，导致拒绝服务等。另外，Linux kernel 被披露存在内存错误引用漏洞。攻击者可利用该漏洞导致发生释放后重用。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、RIOT RIOT-OS 拒绝服务漏洞

验证描述

RIOT RIOT-OS 是一套应用于物联网领域的操作系统。

RIOT 2019.07 及之前版本中的 TCP 实现（gnrc_tcp）存在拒绝服务漏洞，攻击者可利用该漏洞造成无限循环，导致拒绝服务。

验证信息

POC 链接：https://github.com/RIOT-OS/RIOT/issues/12086

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2019-47025

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. 研究员发现 Twitter 安卓应用漏洞

12 月 26 日，据 TechCrunch 消息，安全研究员 Ibrahim Balic 称，利用 Twitter 安卓应用程序中的一个漏洞，将 1700 万个电话号码与 Twitter 用户帐户进行了匹配，并且可以通过 Twitter 的联系人上传功能上传生成的全部电话号码列表。

参考链接：https://www.bianews.com/news/details?id=49972

2. 谷歌浏览器受新的 Magellan 2.0 漏洞影响

腾讯刀锋安全团队披露了一组新的 SQLite 漏洞”Magellan 2.0”，该漏洞允许攻击者在谷歌 Chrome 浏览器上运行恶意代码。漏洞共有五个，所有使用 SQLite 数据库的应用程序都容易受到 Magellan 2.0 的攻击。

参考链接：https://www.zdnet.com/article/google-chrome-impacted-by-new-magellan-2-0-vulnerabilities/

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