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 09 日-2019 年 12 月 15 日 **2019 年第 50 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 327 个，其中高危漏洞 133 个、中危漏洞 172 个、低危漏洞 22 个。漏洞平均分值为 6.15。本周收录的漏洞中，涉及 0day 漏洞 120 个（占 37%），其中互联网上出现“WordPress CSS Hero 插件跨站脚本漏洞、Intelbras WRN 150 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 2695 个，与上周（2338 个）环比增长 15%。

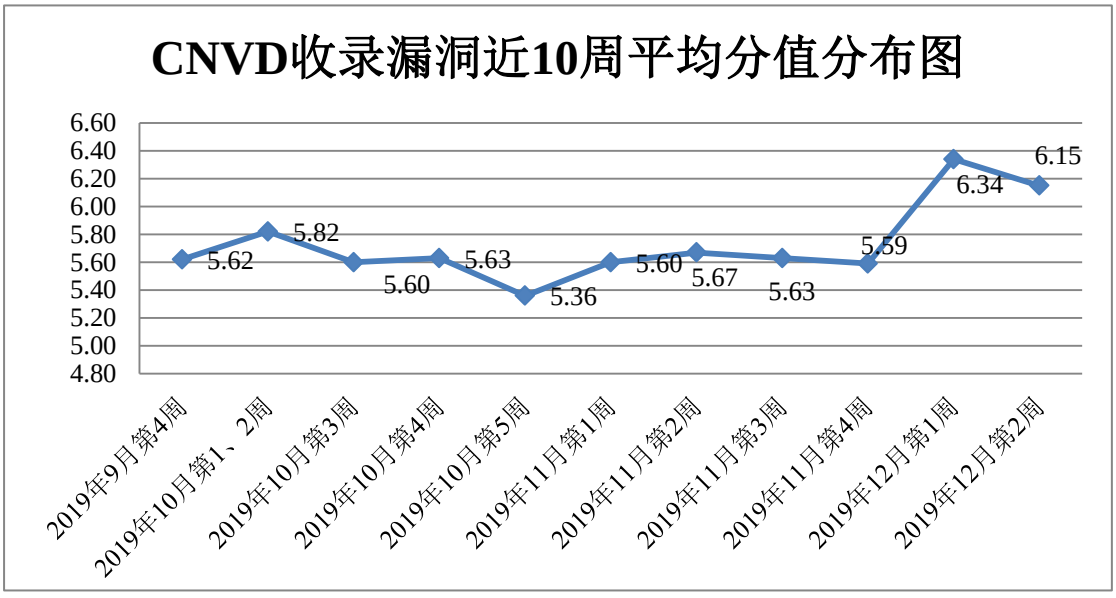

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 7 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 213 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 40 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 14 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：

沧州市凡诺广告传媒有限公司、长沙米拓信息技术有限公司、南充市老虎云网络技术有限公司、山西企凝信息科技有限公司、西安旭阳信息技术有限公司、上海祥虹信息技术有限公司、大庆久久网络科技有限公司、广州永拓信息科技有限公司、无锡时光网络科技有限公司、北京椒图科技有限公司、大连图扑物联科技有限公司、北京超越无限信息技术有限公司、青岛易软天创网络科技有限公司、中铁置业集团有限公司、西安动力无限信息技术有限公司、宁波智慧天成品牌策划有限公司、华米（北京）信息科技有限公司、铭飞科技有限公司、廊坊市极致网络科技有限公司、广州齐博网络科技有限公司、云络电子科技有限公司、衡水金航计算机科技有限公司、上海圆通速递有限公司、四川省新悦网络信息技术服务有限公司、北京良精志诚科技有限责任公司、深圳市迪元素科技有限公司、深圳市锟铻科技有限公司、上海亿速网络科技有限公司、安徽省科迅教育装备有限公司、常州市盛科网络科技有限公司、汕头市三互科技有限公司、济南有人物联网技术有限公司、歐耶資訊有限公司、鞍钢招标有限公司、北京得安信息技术有限公司、北京金盘软件技术有限公司、睿谷信息科技有限公司、上海春风物流股份有限公司、成都鹏博士电信传媒集团股份有限公司、北京文网亿联科技有限公司、佳能（中国）有限公司、金华市激石信息技术有限公司、深圳市龙腾盛世科技有限公司、抚顺市经纬网络技术开发有限公司、上海待迩信息科技有限公司、金华飞狐网络科技有限公司、海南赞赞网络科技有限公司、中国民主法治出版社、棠下互联、长江勘测规划设计研究院、乐尚商城开源系统、网新科技、中国环境科学学会、苹果 CMS、海洋 CMS、5iSNS 实验室、极致 CMS、Emlog、ZZZCMS、HYBBS、HisiPHP、SeaCMS、HongCMS 和 HadSky。

本周，CNVD 发布了《Microsoft 发布 2019 年 12 月安全更新》。详情参见 CNVD 网站公告内容。

https://www.cnvd.org.cn/webinfo/show/5323

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、北京知道创宇信息技术股份有限公司、恒安嘉新(北京)科技股份公司等单位报送公开收集的漏洞数量较多。西门子（中国）有限公司、内蒙古洞明科技有限公司、内蒙古奥创科技有限公司、山东新潮信息技术有限公司、国瑞数码零点实验室、远江盛邦（北京）网络安全科技股份有限公司、南京众智维

信息科技有限公司、河南灵创电子科技有限公司 、杭州迪普科技股份有限公司、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、新疆海狼科技有限公司、北京华云安信息技术有限公司、北京长亭科技有限公司、广州蕴辰网络科技有限公司、京东云安全、山东华鲁科技发展股份有限公司、上海端御信息科技有限公司、北京圣博润高新技术股份有限公司、江苏保旺达软件技术有限公司、厦门靠谱云股份有限公司、国家互联网应急中心、山石网科通信技术股份有限公司、郑州赛欧思科技有限公司、河南信安世纪科技有限公司、北京智游网安科技有限公司、国网思极检测技术（北京）有限公司、安吉加加信息技术有限公司、上海并擎软件科技有限公司及其他个人白帽子向CNVD提交了2695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1832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）	891	891
斗象科技（漏洞盒子）	476	476
上海交大	465	465
北京天融信网络安全技术有限公司	265	1
哈尔滨安天科技集团股份有限公司	211	0
华为技术有限公司	192	0
北京知道创宇信息技术股份有限公司	107	107
恒安嘉新(北京)科技股份公司	82	0
北京神州绿盟科技有限公司	73	0
深信服科技股份有限公司	69	1
四川无声信息技术有限公司	69	69
北京启明星辰信息安全技术有限公司	45	0
厦门服云信息科技有限公司	31	9
中国电信集团系统集成有限责任公司	30	30

新华三技术有限公司	23	0
北京数字观星科技有限公司	19	0
深圳市腾讯计算机系统有限公司（玄武实验室）	15	15
南京联成科技发展股份有限公司	4	4
腾讯安全云鼎实验室	1	0
西门子（中国）有限公司	70	0
内蒙古洞明科技有限公司	62	62
内蒙古奥创科技有限公司	46	46
山东新潮信息技术有限公司	33	33
国瑞数码零点实验室	30	30
远江盛邦（北京）网络安全科技股份有限公司	30	30
南京众智维信息科技有限公司	24	24
河南灵创电子科技有限公司	22	22
杭州迪普科技股份有限公司	17	3
杭州海康威视数字技术股份有限公司	17	17
山东云天安全技术有限公司	16	16
新疆海狼科技有限公司	8	8
北京华云安信息技术有限公司	7	7
北京长亭科技有限公司	4	4
广州蕴辰网络科技有限公司	3	3
京东云安全	3	3
山东华鲁科技发展股份有限公司	3	3

上海端御信息科技有限公司	2	2
北京圣博润高新技术股份有限公司	2	2
江苏保旺达软件技术有限公司	1	1
厦门靠谱云股份有限公司	1	1
国家互联网应急中心	1	1
山石网科通信技术股份有限公司	1	1
郑州赛欧思科技有限公司	1	1
河南信安世纪科技有限公司	1	1
北京智游网安科技有限公司	1	1
国网思极检测技术（北京）有限公司	1	1
安吉加加信息技术有限公司	1	1
上海并擎软件科技有限公司	1	1
CNCERT 天津分中心	18	18
CNCERT 甘肃分中心	2	2
个人	282	282
报送总计	3779	2695

本周漏洞按类型和厂商统计

本周，CNVD 收录了 327 个漏洞。应用程序 184 个，WEB 应用 70 个，操作系统 35 个，智能设备（物联网终端设备）17 个，网络设备（交换机、路由器等网络端设备）17 个，安全产品 3 个和数据库 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	184
WEB 应用	70
操作系统	35

智能设备（物联网终端设备）	17
网络设备（交换机、路由器等网络端设备）	17
安全产品	3
数据库	1

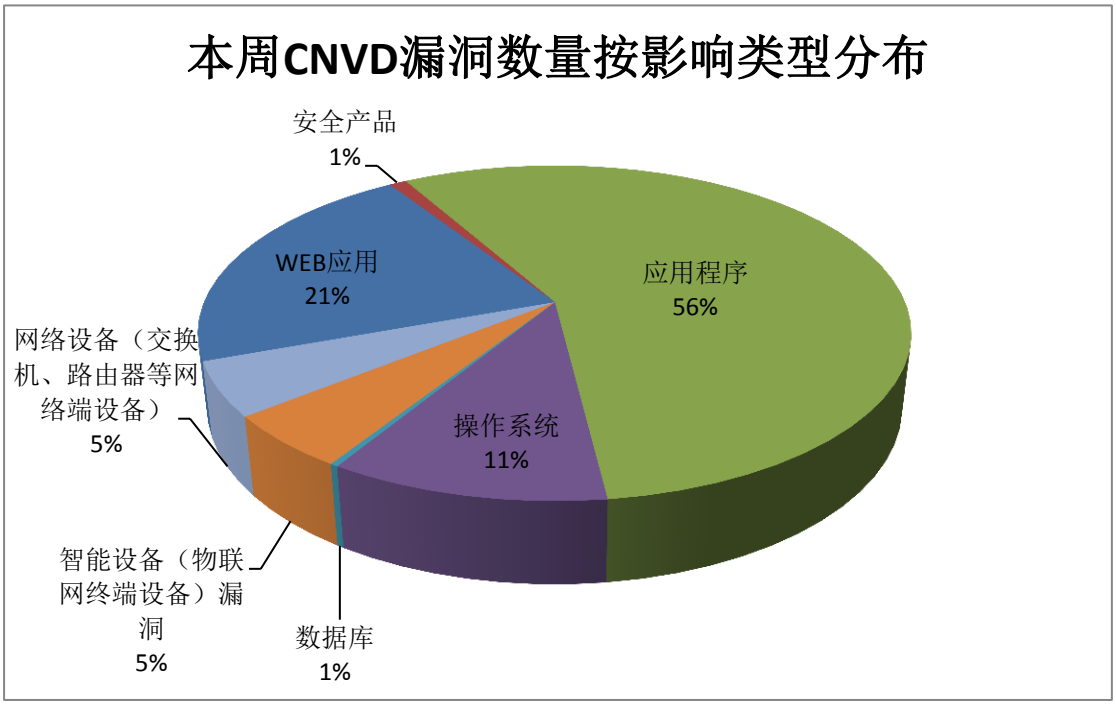

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Siemens、SeaCMS、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	Siemens	26	8%
2	SeaCMS	23	7%
3	IBM	21	6%
4	Google	14	4%
5	Schneider Electric	14	4%
6	Apple	10	3%
7	Huawei	10	3%
8	Red Hat	10	3%
9	Linux	9	3%
10	其他	190	59%

本周行业漏洞收录情况

本周，CNVD 收录了 9 个电信行业漏洞，22 个移动互联网行业漏洞，46 个工控行业漏洞（如下图所示）。其中，“Siemens SiNVR 3 Central Control Server (CCS)目录遍历漏洞、Google Android kernel 权限提升漏洞（CNVD-2019-44506）和 ABB Relion 670 系列路径遍历漏洞、Apple macOS Catalina 内存破坏漏洞（CNVD-2019-44548）、多款 FON 产品输入验证错误漏洞”等漏洞的综合评级为“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/

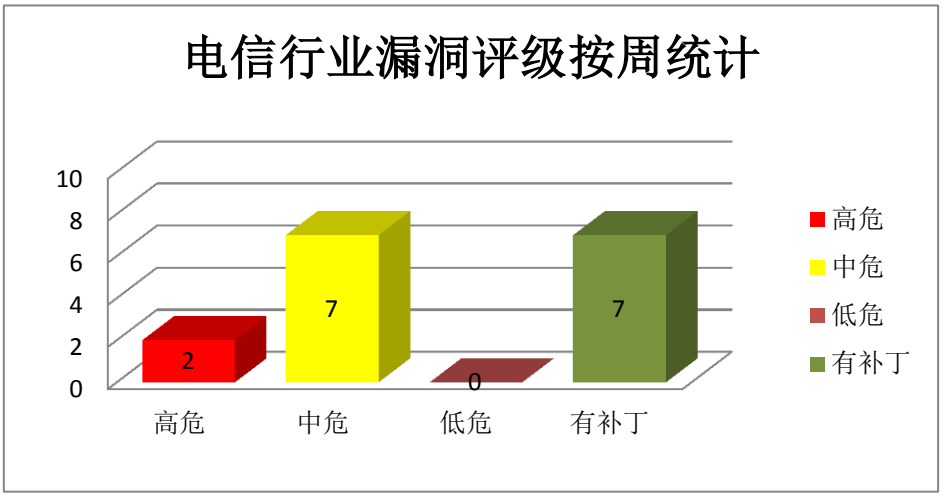

图 3 电信行业漏洞统计

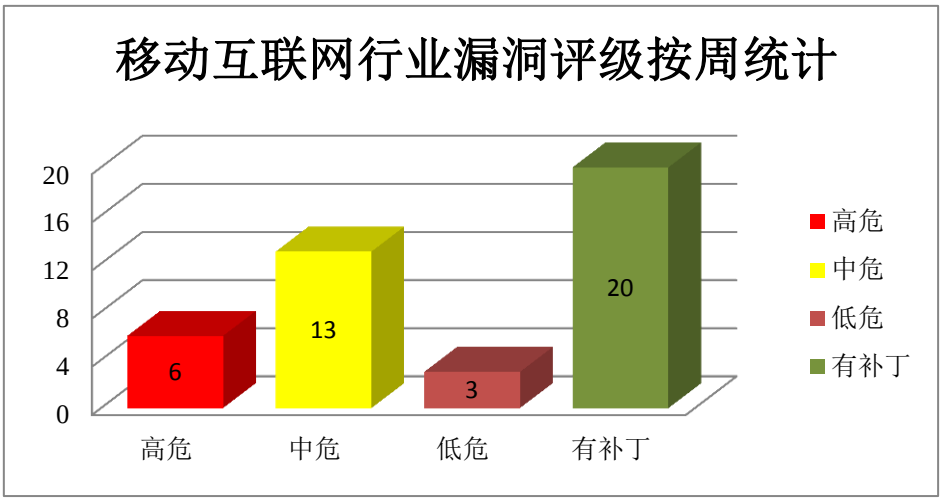

图 4 移动互联网行业漏洞统计

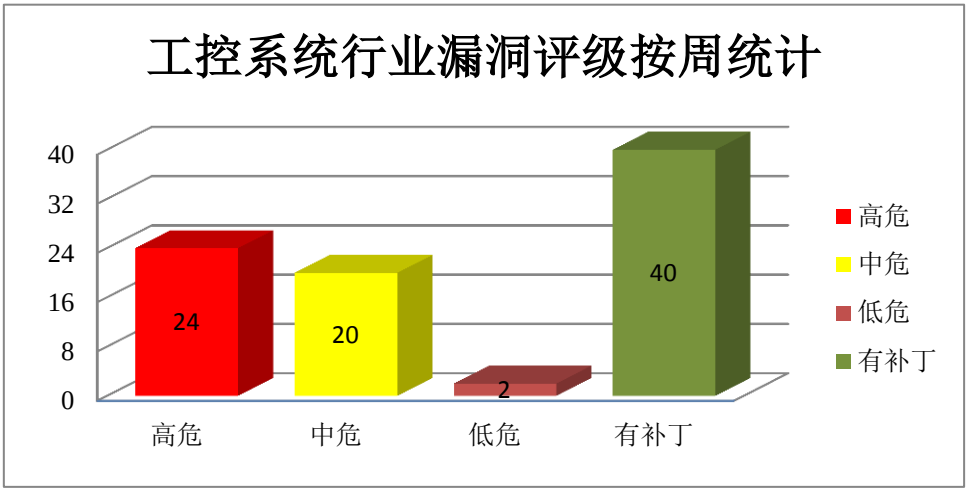

图 5 工控系统行业漏洞统计

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、Siemens 产品安全漏洞

SPPA-T3000 是一种分布式控制系统，主要应用于火力发电厂和大型可再生能源发电厂。本周，上述产品被披露存在堆缓冲区溢出漏洞，攻击者可利用漏洞通过向 5010/tcp 发送精心编制的数据包，造成拒绝服务情况并可获得远程代码执行。

CNVD 收录的相关漏洞包括：Siemens SPPA-T3000 堆缓冲区溢出漏洞（CNVD-2019-44770、CNVD-2019-44773、CNVD-2019-44774、CNVD-2019-44775、CNVD-2019-44776、CNVD-2019-44778、CNVD-2019-44779、CNVD-2019-44780）。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-2019-44770

http://www.cnvd.org.cn/flaw/show/CNVD-2019-44773

http://www.cnvd.org.cn/flaw/show/CNVD-2019-44774

http://www.cnvd.org.cn/flaw/show/CNVD-2019-44775

http://www.cnvd.org.cn/flaw/show/CNVD-2019-44776

http://www.cnvd.org.cn/flaw/show/CNVD-2019-44778

http://www.cnvd.org.cn/flaw/show/CNVD-2019-44779

http://www.cnvd.org.cn/flaw/show/CNVD-2019-44780

2、IBM 产品安全漏洞

IBM Planning Analytics 是美国 IBM 公司的一套业务规划分析解决方案。IBM Rational Collaborative Lifecycle Management（CLM）是一套协作化生命周期管理解决方案。IBM API Connect（APIConnect）是一套用于管理 API 生命周期的集成解决方案。IBM

PureApplication System 是一套专为事务性 Web 和数据库应用程序而设计的平台系统。IBM Cloud Pak System 是一套具有可配置、预集成软件的全栈、融合基础架构。IBM Spectrum Protect 是一套数据保护平台。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞注入任意 JavaScript 代码，执行未授权操作，提升权限，查看任意文件，获取敏感信息。

CNVD 收录的相关漏洞包括：IBM Planning Analytics 跨站脚本漏洞（CNVD-2019-44562）、IBM Rational Collaborative Lifecycle Management 路径遍历漏洞、IBM API Connect 信息泄露漏洞（CNVD-2019-44943、CNVD-2019-44942）、IBM PureApplication System 信息泄露漏洞（CNVD-2019-44944）、IBM Cloud Pak System 跨站请求伪造漏洞、IBM Spectrum Protect Servers 和 Storage Agents 权限许可和访问控制问题漏洞、IBM API Connect 日志信息泄露漏洞。其中，“IBM Cloud Pak System 跨站请求伪造漏洞、IBM Spectrum Protect Servers 和 Storage Agents 权限许可和访问控制问题漏洞”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-2019-44562

http://www.cnvd.org.cn/flaw/show/CNVD-2019-44940

http://www.cnvd.org.cn/flaw/show/CNVD-2019-44943

http://www.cnvd.org.cn/flaw/show/CNVD-2019-44942

http://www.cnvd.org.cn/flaw/show/CNVD-2019-44944

http://www.cnvd.org.cn/flaw/show/CNVD-2019-44974

http://www.cnvd.org.cn/flaw/show/CNVD-2019-44989

http://www.cnvd.org.cn/flaw/show/CNVD-2019-44991

3、Apple 产品安全漏洞

Apple macOS Catalina 是美国苹果（Apple）公司的一套专为 Mac 计算机所开发的专用操作系统。manpages 是其中的一个系统手册组件。UIFoundation 是其中的一个 UI 框架组件。CUPS 是其中的一个开源的用于 OS X 和类 Unix 系统的打印系统组件。File Quarantine 是其中的一个文件隔离组件。IOGraphics 是其中的一个输入输出显卡组件。libxml2 是其中的一个基于 C 语言的用来解析 XML 文档的函数库组件。Apple iTunes for Windows 是一款基于 Windows 平台的媒体播放器应用程序。Apple iOS 是一套为移动设备所开发的操作系统。Apple tvOS 是一套智能电视操作系统。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，攻击者可利用漏洞获取 root 权限，执行任意代码，造成拒绝服务等。

CNVD 收录的相关漏洞包括：Apple macOS Catalina 权限提升漏洞、Apple macOS Catalina 信息泄露漏洞、Apple tvOS、Apple iOS 和 Apple iPadOS UIFoundation 组件缓冲区溢出漏洞、Apple macOS Catalina 拒绝服务漏洞、Apple macOS Catalina File Q

uarantine 组件权限提升漏洞、Apple macOS Catalina 和 Apple iTunes for Windows 动态库加载漏洞、Apple macOS Catalina IOGraphics 组件缓冲区溢出漏洞、Apple macOS Catalina 内存破坏漏洞（CNVD-2019-44548）。其中，除“Apple macOS Catalina 信息泄露漏洞，Apple macOS Catalina 拒绝服务漏洞，Apple macOS Catalina File Quarantine 组件权限提升漏洞”外的漏洞综合评级为“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-2019-44539
http://www.cnvd.org.cn/flaw/show/CNVD-2019-44541
http://www.cnvd.org.cn/flaw/show/CNVD-2019-44543
http://www.cnvd.org.cn/flaw/show/CNVD-2019-44544
http://www.cnvd.org.cn/flaw/show/CNVD-2019-44545
http://www.cnvd.org.cn/flaw/show/CNVD-2019-44546
http://www.cnvd.org.cn/flaw/show/CNVD-2019-44547
http://www.cnvd.org.cn/flaw/show/CNVD-2019-44548

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。kernel 是其中的一个内核。VL53L0 driver 是其中的一个激光测距传感器。I2C driver 是其中的一个两线式串行总线驱动程序。USB driver 是其中的一个通用串行总线（USB）驱动程序。Google Chrome 是一款 Web 浏览器。Blink 是美国谷歌（Google）公司和挪威欧朋（OperaSoftware）公司共同开发的一套浏览器排版引擎（渲染引擎）。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。

CNVD 收录的相关漏洞包括：Google Android kernel 权限提升漏洞（CNVD-2019-44505、CNVD-2019-44506）、Google Chrome Blink 资源管理错误漏洞（CNVD-2019-44525、CNVD-2019-44526、CNVD-2019-44527）、Google Android VL53L0 驱动程序权限提升漏洞、Google Android I2C 驱动程序权限提升漏洞、Google Android USB 驱动程序权限提升漏洞。其中，“Google Android kernel 权限提升漏洞（CNVD-2019-44506）”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-2019-44505
http://www.cnvd.org.cn/flaw/show/CNVD-2019-44506
http://www.cnvd.org.cn/flaw/show/CNVD-2019-44525
http://www.cnvd.org.cn/flaw/show/CNVD-2019-44526
http://www.cnvd.org.cn/flaw/show/CNVD-2019-44527
http://www.cnvd.org.cn/flaw/show/CNVD-2019-44731

http://www.cnvd.org.cn/flaw/show/CNVD-2019-44732

http://www.cnvd.org.cn/flaw/show/CNVD-2019-44730

5、Linux kernel 本地拒绝服务漏洞（CNVD-2019-44555）

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。本周，Linux kernel 被披露存在本地拒绝服务漏洞。攻击者可利用该漏洞造成拒绝服务。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-2019-44555

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-2019-44549	Red Hat OpenShift Container Platform 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://github.com/openshift/openshift-ansible/pull/11860
CNVD-2019-44559	Huawei Honor Play 信息泄露漏洞	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-20191127-02-smartphone-cn
CNVD-2019-44727	QNAP Systems QNAP Music Station 跨站脚本漏洞	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.qnap.com/zh-tw/security-advisory/nas-201911-27
CNVD-2019-44758	VMware Harbor Container Registry for Pivotal Platform SQL 注入漏洞	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/goharbor/harbor/security/advisories/GHSA-rh89-vvrg-fg64
CNVD-2019-44955	Fuji Electric Energy Savings Estimator DLL 加载本地代码执行漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://ics-cert.us-cert.gov/advisories/ICSA-18-282-07
CNVD-2019-45002	Cisco Unity Express 操作系统命令注入漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191120-unity-exp-comm-inject
CNVD-2019-45135	Dell EMC Storage Monitoring and Reporting 代码问题漏洞	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.dell.com/support/security/z

			h-cn/details/538977/DSA-2019-176-Dell-EMC-Storage-Monitoring-and-Reporting-SMR-Java-RMI-Deserialization-of-Untruste
CNVD-2019-45154	Mozilla Network Security Services 拒绝服务漏洞	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://github.com/nss-dev/nss
CNVD-2019-45164	Fronius Solar Inverter Series 后门账户漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：http：//www.fronius.com
CNVD-2019-45327	SUSE Mailman 权限提升漏洞	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.gnu.org/software/mailman/

小结：本周，Siemens 产品被披露存在堆缓冲区溢出漏洞，攻击者可利用漏洞通过向 5010/tcp 发送精心编制的数据包，造成拒绝服务情况并可获得远程代码执行。此外，IBM、Apple、Google 等多款产品被披露存在多个漏洞，攻击者可利用漏洞注入任意 JavaScript 代码，获取敏感信息，提升权限，执行任意代码，造成拒绝服务。另外，Linux kernel 被披露存在本地拒绝服务漏洞。攻击者可利用该漏洞造成拒绝服务。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、Intelbras WRN 150 跨站请求伪造漏洞

验证描述

Intelbras WRN 150 是波兰 Intelbras 公司的一款无线路由器。

Intelbras WRN 150 1.0.18 版本中存在跨站请求伪造漏洞。攻击者可利用该漏洞更改密码。

验证信息

POC 链接：https://packetstormsecurity.com/files/155557/Intelbras-Router-RF1200-1.1.3-Cross-Site-Request-Forgery.html

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2019-45151

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. Mozilla 将要求所有扩展开发者启用双重认证

扩展社区经理 Caitlin Neiman 称，从 2020 年初开始，扩展开发者将要求在扩展网站 AMO（Mozilla Add-Ons）对其账号启用 2FA，此举旨在防止恶意攻击者控制合法扩展及其用户。如果攻击者控制了扩展开发者的账号，他们可以向 Firefox 用户推送恶意更新，如窃取密码，监视用户浏览习惯，或重定向用户到钓鱼或恶意程序下载站。此类攻击通常被称为供应链攻击。

参考链接：https://www.solidot.org/story?sid=62936

2. Elementor 和 Beaver 插件中的漏洞让任何人能轻易破解 WordPress 网站

安全研究人员已经在两个广泛使用的高级 WordPress 插件中发现了一个关键但易于利用的身份验证绕过漏洞，该漏洞可能使远程攻击者无需任何密码即可获得对站点的管理访问权限。

参考链接：https://thehackernews.com/2019/12/wordpress-elementor-beaver.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