国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2020 年 11 月 02 日-2020 年 11 月 08 日　　2020 年第 45 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 340 个，其中高危漏洞 113 个、中危漏洞 167 个、低危漏洞 60 个。漏洞平均分值为 6.00。本周收录的漏洞中，涉及 0day 漏洞 96 个（占 28%），其中互联网上出现“Victor CMS 跨站脚本漏洞（CNVD-2020-61026）、kkcms 存在存储型跨站脚本漏洞”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 3727 个，与上周（9867 个）环比减少 62%。

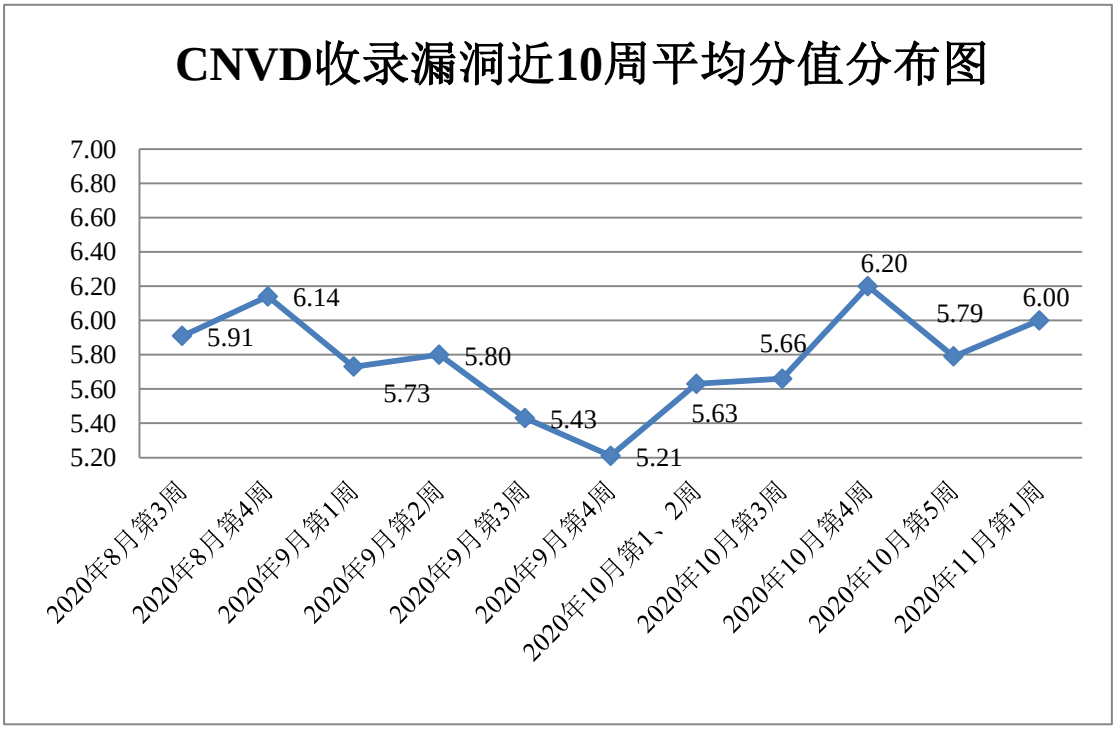

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 9 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 481 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 119 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 32 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：

小米科技有限责任公司、沈阳点动科技有限公司、北京用友政务软件股份有限公司、用友网络科技股份有限公司、淄博闪灵网络科技有限公司、漳州盾灵网络科技有限公司、北京海腾时代科技有限公司、上海商创网络科技有限公司、青岛易企天创管理咨询有限公司、邯郸开发区图布斯软件技术有限公司、上海晓材科技有限公司、洛阳云业信息科技有限公司、北京良精志诚科技有限责任公司、中国中铁建工集团有限公司、北京国炬信息技术有限公司、方法数码（成都）科技有限公司、廊坊市极致网络科技有限公司、山西山大新网科技有限公司、深圳市简芯科技有限公司、天津南大通用数据技术股份有限公司、广州齐博网络科技有限公司、厦门天锐科技股份有限公司、北京臻鼎科技有限公司、武汉创益云信息技术有限公司、北京中成科信科技发展有限公司、广州安网通信技术有限公司、杭州吉拉科技有限公司、上海展盟网络科技有限公司、长沙市同迅计算机科技有限公司、锐捷网络股份有限公司、西安众邦网络科技有限公司、四川思途智旅软件有限公司、深圳市普燃计算机软件科技有限公司、北京微步在线科技有限公司、杭州新视窗信息技术有限公司、深圳市杰源网络信息有限公司、昆明紫电科技发展有限公司、深圳市拓普泰尔科技有限公司、上海互联网软件集团有限公司、天津市华易动力信息科技有限公司、华硕电脑（上海）有限公司、上海互盾信息科技有限公司、北京致远互联软件股份有限公司、倾天网络科技（上海）有限公司、重庆猫扑网络科技有限公司、昆明云涛科技有限公司、成都依能科技股份有限公司、四创科技有限公司、成都海之螺科技有限公司、西门子（中国）有限公司、镇江市云优网络科技有限公司、霍尼韦尔（中国）有限公司、上海纵之格科技有限公司、上海卓卓网络科技有限公司、广东德生科技股份有限公司、北京辰信领创信息技术有限公司、上海荃路软件开发工作室、沈阳市皇姑区爱浓网络技术服务中心、若依、新秀工作室、ZZCMS、Hancom、Projectworlds、BEESCMS 和 kkcms。

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，阿里云计算有限公司、北京天融信网络安全技术有限公司、北京神州绿盟科技有限公司、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、北京华顺信安科技有限公司、山东新潮信息技术有限公司、山东云天安全技术有限公司、北京天

地和兴科技有限公司、北京华云安信息技术有限公司、河南灵创电子科技有限公司 、河南信安世纪科技有限公司、山东华鲁科技发展股份有限公司、杭州迪普科技股份有限公司、北京机沃科技有限公司、北京云科安信科技有限公司（Seraph 安全实验室）、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、内蒙古奥创科技有限公司、山东道普测评技术有限公司、泰山信息科技有限公司、山东正中信息技术股份有限公司、杭州海康威视数字技术股份有限公司、广州市蓝爵计算机科技有限公司、安徽长泰信息安全服务有限公司、北京零零信安科技有限公司、山石网科通信技术股份有限公司、上海观安信息技术股份有限公司、国家互联网应急中心、北京长亭科技有限公司、京东云安全、平安银河实验室、四川哨兵信息科技有限公司、北京安华金和科技有限公司、北京智游网安科技有限公司、北京惠而特科技有限公司、北京锐服信科技有限公司、江苏保旺达软件技术有限公司、上海纽盾科技股份有限公司、上海市信息安全测评认证中心、武汉安域信息安全技术有限公司及其他个人白帽子向 CNVD 提交了 3727 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 2371 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）	1365	1365
安信网神（补天平台）	573	573
上海交大	433	433
阿里云计算有限公司	483	0
北京天融信网络安全技术有限公司	463	3
北京神州绿盟科技有限公司	353	48
哈尔滨安天科技集团股份有限公司	210	0
深信服科技股份有限公司	177	0
新华三技术有限公司	134	0
华为技术有限公司	106	0
北京数字观星科技有限公司	62	0
北京启明星辰信息安全技术有限公司	59	1

中新网络信息安全股份有限公司	26	26
中国电信集团系统集成有限责任公司	14	14
北京知道创宇信息技术股份有限公司	12	0
腾讯安全云鼎实验室	3	0
北京奇虎科技有限公司	1	1
国瑞数码零点实验室	269	269
北京华顺信安科技有限公司	122	1
山东新潮信息技术有限公司	74	74
山东云天安全技术有限公司	31	31
北京天地和兴科技有限公司	30	30
北京华云安信息技术有限公司	28	28
河南灵创电子科技有限公司	27	27
河南信安世纪科技有限公司	26	26
山东华鲁科技发展股份有限公司	19	19
杭州迪普科技股份有限公司	14	14
北京机沃科技有限公司	10	10
北京云科安信科技有限公司（Seraph 安全实验室）	10	10
远江盛邦（北京）网络安全科技股份有限公司	10	10
南京众智维信息科技有限公司	8	8
内蒙古奥创科技有限公司	7	7
山东道普测评技术有限公司	7	7
泰山信息科技有限公司	7	7
山东正中信息技术股份有限	6	6

公司		
杭州海康威视数字技术股份有限公司	4	4
广州市蓝爵计算机科技有限公司	4	4
安徽长泰信息安全服务有限公司	4	4
北京零零信安科技有限公司	4	4
山石网科通信技术股份有限公司	4	4
上海观安信息技术股份有限公司	4	4
国家互联网应急中心	4	4
北京长亭科技有限公司	3	3
京东云安全	3	3
平安银河实验室	3	3
四川哨兵信息科技有限公司	3	3
北京安华金和科技有限公司	2	2
北京智游网安科技有限公司	1	1
北京惠而特科技有限公司	1	1
北京锐服信科技有限公司	1	1
江苏保旺达软件技术有限公司	1	1
上海纽盾科技股份有限公司	1	1
上海市信息安全测评认证中心	1	1
武汉安域信息安全技术有限公司	1	1
CNCERT 宁夏分中心	9	9
CNCERT 四川分中心	5	5
CNCERT 浙江分中心	2	2

CNCERT 上海分中心	1	1
个人	613	613
报送总计	5858	3727

本周漏洞按类型和厂商统计

本周，CNVD 收录了 340 个漏洞。应用程序 194 个，WEB 应用 74 个，操作系统 46 个，网络设备（交换机、路由器等网络端设备）14 个，智能设备（物联网终端设备）漏洞 6 个，数据库 4 个，安全产品 2 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	194
WEB 应用	74
操作系统	46
网络设备（交换机、路由器等网络端设备）	14
智能设备（物联网终端设备）	6
数据库	4
安全产品	2

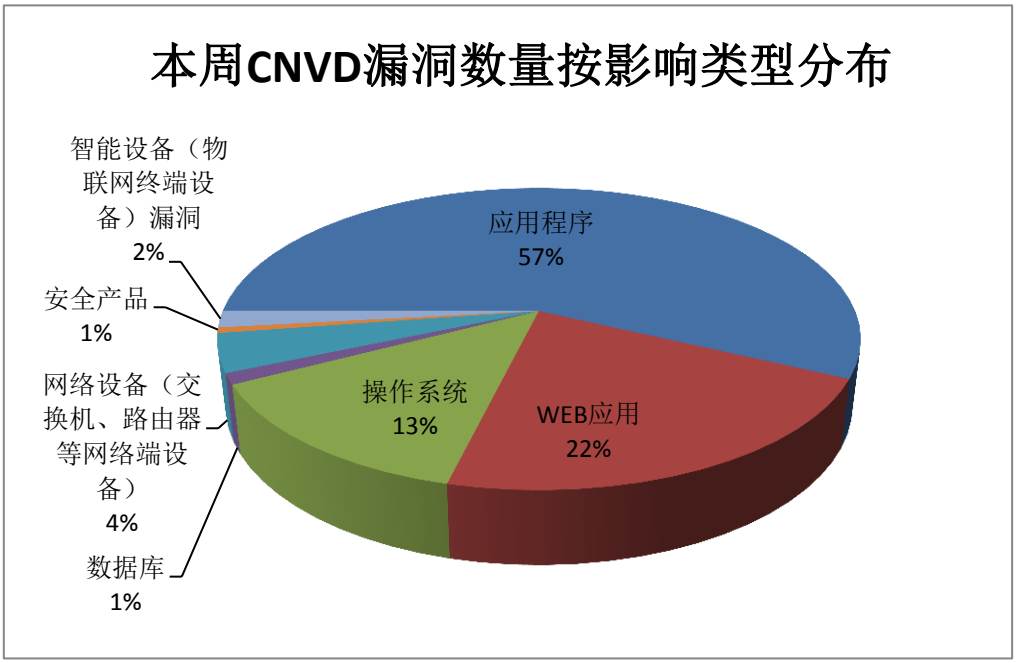

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Oracle、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	Oracle	44	13%
2	Google	34	10%
3	Apple	22	6%
4	Adobe	15	5%
5	Pulse Secure	12	4%
6	Synology	11	3%
7	深圳市惟新控股有限合伙企业	11	3%
8	IBM	10	3%
9	Microsoft	10	3%
10	其他	171	50%

本周行业漏洞收录情况

本周，CNVD 收录了 27 个电信行业漏洞，26 个移动互联网行业漏洞，9 个工控行业漏洞（如下图所示）。其中，“Apple AirPort Base Station 代码问题漏洞（CNVD-2020-60818）、Apple AirPort Base Station 资源管理错误漏洞、Oracle WebLogic Server 远程代码执行漏洞（CNVD-2020-61040）、Synology Router Manager 信任管理问题漏洞”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/

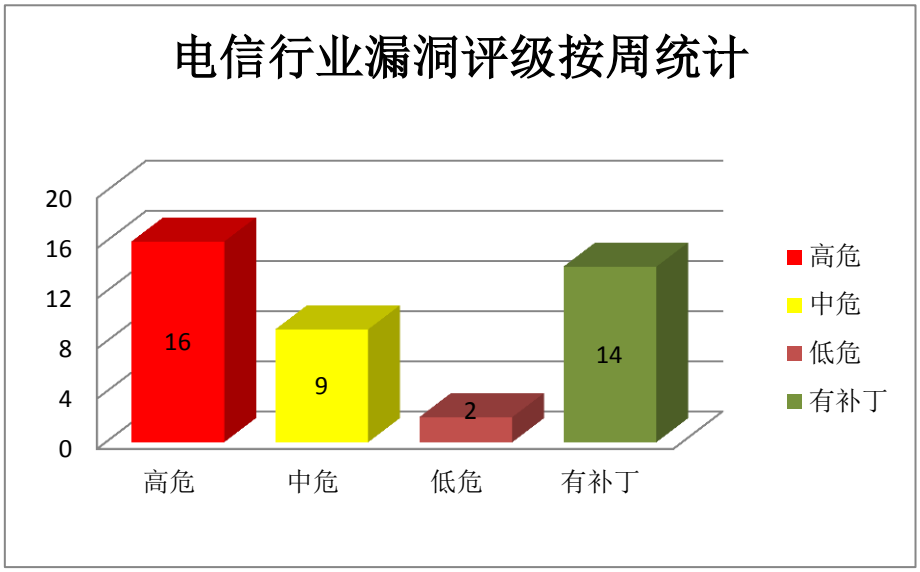

图 3 电信行业漏洞统计

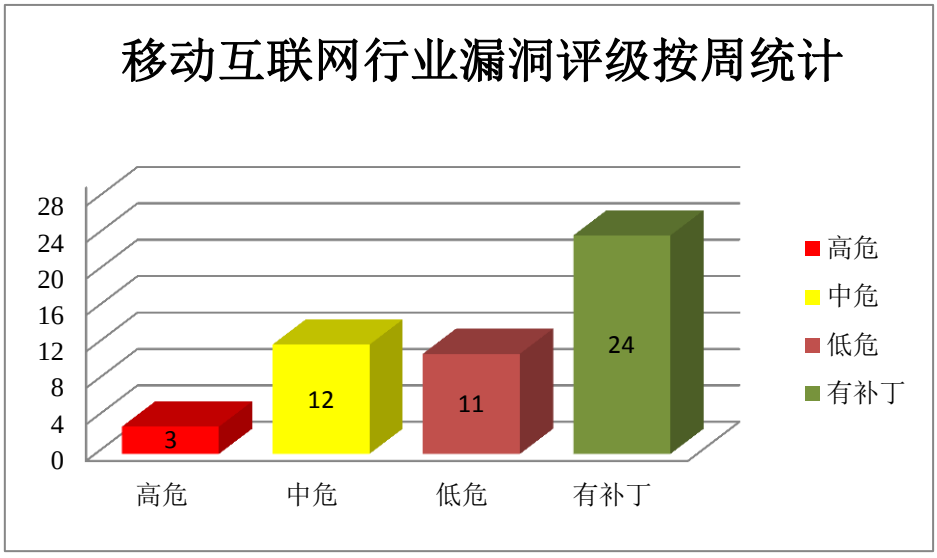

图 4 移动互联网行业漏洞统计

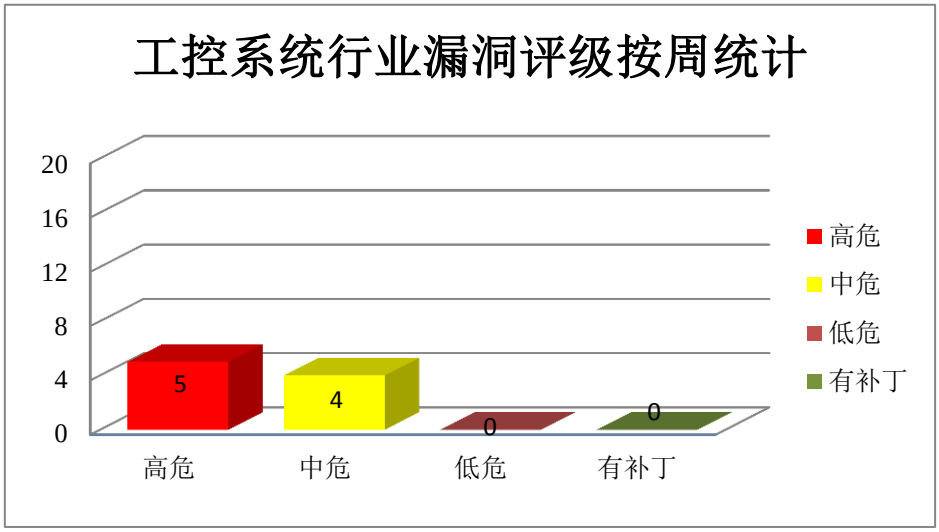

图 5 工控系统行业漏洞统计

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、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。Apple macOS Mojave 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。Apple AirPort Base Station 是美国苹果（Apple）公司的一款无线路由器。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞造成拒绝服务，缓冲区溢出或堆溢出，执行任意代码等。

CNVD 收录的相关漏洞包括：Apple macOS Catalina 缓冲区溢出漏洞（CNVD-2020-60815、CNVD-2020-61020、CNVD-2020-60814）、Apple macOS Mojave 缓冲区溢出漏洞、Apple AirPort Base Station 资源管理错误漏洞、Apple AirPort Base Station 代码问题漏洞（CNVD-2020-60818、CNVD-2020-60820）、Apple macOS Catalina 竞争条件问题漏洞。其中，“Apple macOS Catalina 缓冲区溢出漏洞（CNVD-2020-60815、CNVD-2020-61020）、Apple macOS Mojave 缓冲区溢出漏洞、Apple AirPort Base Station 资源管理错误漏洞、Apple AirPort Base Station 代码问题漏洞（CNVD-2020-60818、CNVD-2020-60820）”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：https://www.cnvd.org.cn/flaw/show/CNVD-2020-60815
https://www.cnvd.org.cn/flaw/show/CNVD-2020-60821
https://www.cnvd.org.cn/flaw/show/CNVD-2020-60820
https://www.cnvd.org.cn/flaw/show/CNVD-2020-60819
https://www.cnvd.org.cn/flaw/show/CNVD-2020-60818
https://www.cnvd.org.cn/flaw/show/CNVD-2020-61020
https://www.cnvd.org.cn/flaw/show/CNVD-2020-60725
https://www.cnvd.org.cn/flaw/show/CNVD-2020-60814

2、IBM 产品安全漏洞

IBM i2 Analysts Notebook 是美国 IBM 公司的一款数据可视化分析工具。IBM i2 iBase 是一款直观的情报数据管理应用。IBM Sterling External Authentication Server 是美国 IBM 公司的一款客户端应用程序。IBM System x servers 是美国国际商业机器公司（IBM）的一款服务器。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞从浏览器中返回的详细技术错误消息中获取敏感信息，消耗内存资源，在系统上执行任意代码等。

CNVD 收录的相关漏洞包括：IBM i2 Analysts Notebook 内存破坏漏洞（CNVD-2020-60085、CNVD-2020-60086、CNVD-2020-60087、CNVD-2020-60088）、IBM i2 iBase 代码问题漏洞、IBM i2 iBase 信息泄露漏洞、IBM Sterling External Authentication Server 和 IBM Sterling Secure Proxy 内存破坏漏洞、IBM System x servers 任意代码执行漏洞。其中，“IBM i2 Analysts Notebook 内存破坏漏洞（CNVD-2020-60085、CNVD-2020-60086、CNVD-2020-60087、CNVD-2020-60088）”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：https://www.cnvd.org.cn/flaw/show/CNVD-2020-60085

https://www.cnvd.org.cn/flaw/show/CNVD-2020-60084

https://www.cnvd.org.cn/flaw/show/CNVD-2020-60083

https://www.cnvd.org.cn/flaw/show/CNVD-2020-60088

https://www.cnvd.org.cn/flaw/show/CNVD-2020-60087

https://www.cnvd.org.cn/flaw/show/CNVD-2020-60086

https://www.cnvd.org.cn/flaw/show/CNVD-2020-60337

https://www.cnvd.org.cn/flaw/show/CNVD-2020-60338

3、HPE 产品安全漏洞

HPE Intelligent Management Center 是美国惠普企业公司（Hewlett Packard Enterprise，HPE）的一套网络智能管理中心解决方案。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞实现远程代码执行。

CNVD 收录的相关漏洞包括：HPE Intelligent Management Center (iMC) 授权问题漏洞、HPE Intelligent Management Center (iMC) iccselectrules 表达式语言注入远程代码执行漏洞（CNVD-2020-60129）、HPE Intelligent Management Center (iMC) perfaddormoddevicemonitor 表达式语言注入远程代码执行漏洞（CNVD-2020-60128）、HPE Intelligent Management Center (iMC) ictexpertcsvdownload 表达式语言注入远程代码执行漏洞（CNVD-2020-60127）、HPE Intelligent Management Center (iMC) syslogtempletselectwin 表达式语言注入远程代码执行漏洞（CNVD-2020-60134）、HPE Intelligent Management Center (iMC) legend 表达式语言注入远程代码执行漏洞（CNVD-2020-60133）、HPE Intelligent Management Center (iMC) ByteMessageResource transformEntity 输入验证远程代码执行漏洞、HPE Intelligent Management Center (iMC) AccessMgrServlet className 输入验证远程代码执行漏洞。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：https://www.cnvd.org.cn/flaw/show/CNVD-2020-60130

https://www.cnvd.org.cn/flaw/show/CNVD-2020-60129

https://www.cnvd.org.cn/flaw/show/CNVD-2020-60128

https://www.cnvd.org.cn/flaw/show/CNVD-2020-60127

https://www.cnvd.org.cn/flaw/show/CNVD-2020-60134

https://www.cnvd.org.cn/flaw/show/CNVD-2020-60133

https://www.cnvd.org.cn/flaw/show/CNVD-2020-60132

https://www.cnvd.org.cn/flaw/show/CNVD-2020-60131

4、Google 产品安全漏洞

Chrome 是由 Google 开发的一款设计简单、高效的 Web 浏览工具，其特点是简洁、快速。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。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞通过特制的 HTML 页面执行沙盒转义，进行本地特权升级，在系统上执行任意代码，或导致应用程序崩溃等。

CNVD 收录的相关漏洞包括：Google Chrome 堆缓冲区溢出漏洞（CNVD-2020-60469、CNVD-2020-60471）、Google Android actory reset protection 权限检查漏洞、Google Chrome video 资源管理错误漏洞、Google Chrome V8 实现不当漏洞（CNVD-2020-60470、CNVD-2020-60473）、Google Chrome 释放后重用漏洞（CNVD-2020-60475）、Google Chrome ANGLE 策略执行不足漏洞。其中，“Google Chrome 堆缓冲区溢出漏洞（CNVD-2020-60469、CNVD-2020-60471）、Google Android actory reset protection 权限检查漏洞、Google Chrome video 资源管理错误漏洞”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：https://www.cnvd.org.cn/flaw/show/CNVD-2020-60469

https://www.cnvd.org.cn/flaw/show/CNVD-2020-60471

https://www.cnvd.org.cn/flaw/show/CNVD-2020-60507

https://www.cnvd.org.cn/flaw/show/CNVD-2020-60512

https://www.cnvd.org.cn/flaw/show/CNVD-2020-60470

https://www.cnvd.org.cn/flaw/show/CNVD-2020-60475

https://www.cnvd.org.cn/flaw/show/CNVD-2020-60474

https://www.cnvd.org.cn/flaw/show/CNVD-2020-60473

5、Linux kernel 代码问题漏洞（CNVD-2020-61025）

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 产品被披露存在代码问题漏洞。该漏洞源于网络系统或产品的代码开发过程中存在设计或实现不当的问题，攻击者可以利用此漏洞使用被释放的内存，从而导致拒绝服务或执行自定义代码。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：https://www.cnvd.org.cn/flaw/s

how/CNVD-2020-61025

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-2020-60096	KDE Partition Manager 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://kde.org/info/security/advisory-20201017-1.txt
CNVD-2020-60125	Oracle WebLogic Server Core 代码执行漏洞（CNVD-2020-60125）	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.oracle.com/security-alerts/cpuoct2020.html
CNVD-2020-60318	Apache Shiro 权限绕过漏洞（CNVD-2020-60318）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://shiro.apache.org/download.html
CNVD-2020-60322	halo 路径遍历漏洞	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/halo-dev/halo/issues/418
CNVD-2020-60333	Mozilla Firefox 内存破坏漏洞（CNVD-2020-60333）	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.mozilla.org/en-US/security/advisories/mfsa2020-45/
CNVD-2020-60451	Synology Router Manager 信任管理问题漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.synology.cn/zh-cn/security/advisory/Synology_SA_20_14
CNVD-2020-60827	ZOHO ManageEngine Applications Manager SQL 注入漏洞（CNVD-2020-60827）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.manageengine.com/products/applications_manager/issues.html#v14560
CNVD-2020-60992	Ruckus Networks Ruckus vRioT 信任管理问题漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://support.ruckuswireless.com/security_bulletins/305
CNVD-2020-61003	Adobe Acrobat 和 Reader 释放后重用漏洞（CNVD-2020-61003）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://helpx.adobe.com/security/products/acrobat/apsb20-67.html

CNVD-2020-60328	Western Digital My Cloud 远程代码执行漏洞	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.westerndigital.com/support/productsecurity/wdc-20007-my-cloud-firmware-version-5-04-114

小结：本周，Apple 产品被披露存在多个漏洞，攻击者可利用漏洞造成拒绝服务，缓冲区溢出或堆溢出，执行任意代码等。此外，IBM、HPE、Google 等多款产品被披露存在多个漏洞，攻击者可利用漏洞从浏览器中返回的详细技术错误消息中获取敏感信息，消耗内存资源，在系统上执行任意代码等。另外，Linux kernel 产品被披露存在代码问题漏洞。攻击者可利用该漏洞使用被释放的内存，从而导致拒绝服务或执行自定义代码。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、Victor CMS 跨站脚本漏洞（CNVD-2020-61026）

验证描述

Victor CMS 是尼日利亚 Victor Alagwu 软件开发者的一套开源的内容管理系统。

Victor CMS 2019-02-28 及之前版本中存在跨站脚本漏洞。该漏洞源于 WEB 应用缺少对客户端数据的正确验证。攻击者可利用该漏洞执行客户端代码。

验证信息

POC 链接：https://www.exploit-db.com/exploits/48626

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2020-61026

信息提供者

恒安嘉新(北京)科技股份公司

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. GitHub 源代码疑遭泄漏

TypeScript 的开发者 Resynth 发布题为《GitHub 源代码泄漏》的文章指出，GitHub.com 的所有源代码被公开。

参考链接：https://mp.weixin.qq.com/s/n1ufEVDTun21TDpx2pk8Sg

2. CAPCOM 内部服务器遭入侵 游戏资料疑泄露

日本知名的游戏公司 CAPCOM 称该公司服务器 11 月 2 日遭到第三方未授权访问。这次外部未授权的方位主要集中在公司的邮件及文件服务器，目前尚未发现用户资料和信息被盗取的证据。

参考链接：https://hot.cnbeta.com/articles/game/1049005.htm

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