# 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 30 日-2020 年 12 月 06 日　　2020 年第 49 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 266 个，其中高危漏洞 81 个、中危漏洞 166 个、低危漏洞 19 个。漏洞平均分值为 5.86。本周收录的漏洞中，涉及 0day 漏洞 170 个（占 64%），其中互联网上出现“cxuucms SQL 注入漏洞、Desdev DedeCMS 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 6960 个，与上周（4662 个）环比增加 49%。

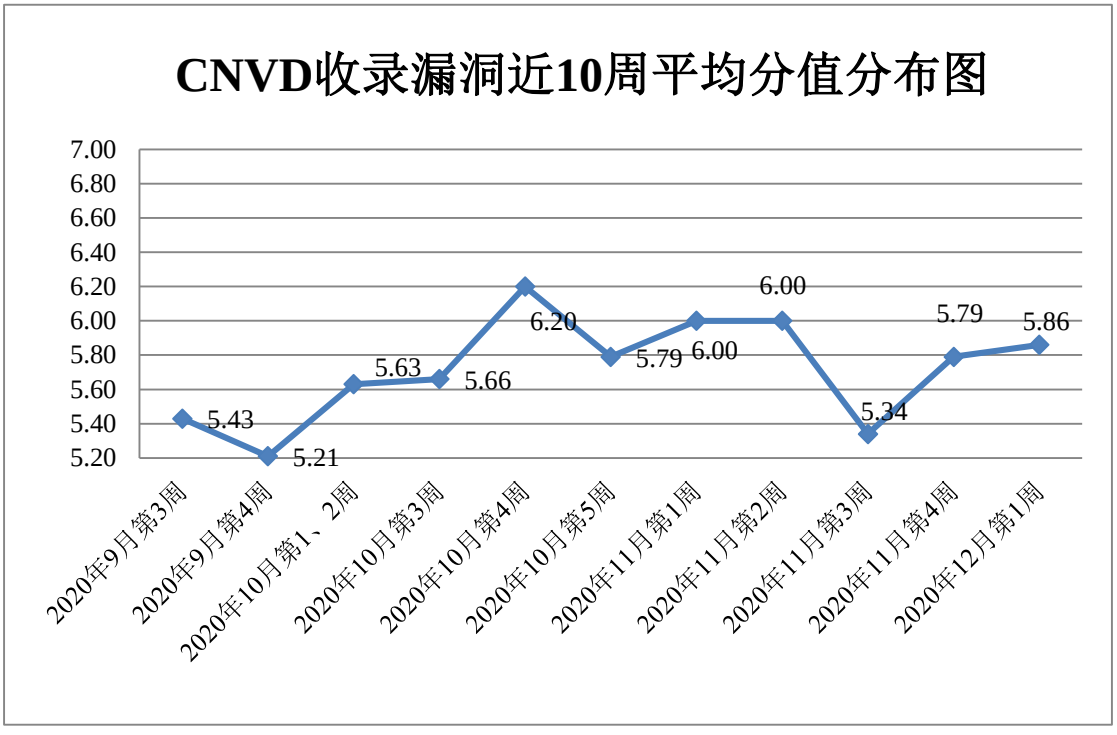


图 1 CNVD 收录漏洞近 10 周平均分值分布图

## 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 34 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 381 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 46 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 66 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：

廊坊市极致网络科技有限公司、北京腾控科技有限公司、重庆亿数信息技术有限公司、北京深度空间装饰工程有限公司、西安信步电子信息技术有限公司、青岛易企天创管理咨询有限公司、上海易正信息技术有限公司、河南天图实业有限公司、昭通灵吉网络科技有限公司、上海秋程信息科技有限公司、哈尔滨伟成科技有限公司、上海商派网络科技有限公司、深圳市锟铻科技有限公司、北京金钥匙凯丽科技发展有限公司、浙江大华技术股份有限公司、联奕科技有限公司、南京帆软软件有限公司、上海炫体信息科技有限公司、长沙友点软件科技有限公司、广东凯格科技有限公司、北京众望网络科技有限公司、长沙米拓信息技术有限公司、南京南软科技有限公司、成都吉胜科技有限责任公司、台州精迅信息技术有限公司、北京中成科信科技发展有限公司、湖北淘码千维信息科技有限公司、北京世纪长秋科技有限公司、太原迅易科技有限公司、深圳市河辰通讯技术有限公司、深圳致软信息技术有限公司、广州易全信息科技有限公司、远江盛邦（北京）网络安全科技股份有限公司、湖南壹拾捌号网络技术有限公司、邳州天目网络科技有限公司、厦门印了么信息科技股份有限公司、苏州浩辰软件股份有限公司、成都依能科技股份有限公司、常州曼好信息技术有限公司、无锡互易科技有限公司、广州亿电邦科智能网络科技有限公司、济南宇霞信息技术有限公司、大庆紫金桥软件技术有限公司、北京汉王精锐科技有限公司、南昌百恒信息技术有限公司、福建福昕软件开发股份有限公司、深圳市瑞吉联通信科技有限公司、三菱电机自动化（中国）有限公司、深圳市中联创新自控系统有限公司、厦门菩提山网络科技有限公司、广东飞企互联科技股份有限公司、嘉兴想天信息科技有限公司、郑州朗创文化传播有限公司、成都易科士信息产业有限公司、福州云钛网络科技有限公司、浙江兰德纵横网路技术股份有限公司、南京三商电脑软件开发有限公司、武汉创益云信息技术有限公司、北京金和网络股份有限公司、用友网络科技股份有限公司、日立产机系统（中国）有限公司、深圳市科图自动化新技术应用公司、广东动易软件股份有限公司、深圳市中达优控科技有限公司、华科网络、佳佳软件、恩平市万商网页设计工作室、若依、蚂蚁笔记、米酷资源网、深圳好生意网络工作室、SIXNET 公司、海洋 CMS、奇乐 CMS、鱼跃 CMS 、华夏 ERP、稻草人 cms 、ThinkAdmin、lzcms、seacms、Z-Blog、KernelApps、Adobe、Nagios、UCMS、MongoDB、CatfishCMS 和 ZZCMS。

## 本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，哈尔滨安天科技集团股份有限公司、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、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。山东新潮信息技术有限公司、山东云天安全技术有限公司、远江盛邦（北京）网络安全科技股份有限公司、北京天地和兴科技有限公司、河南灵创电子科技有限公司、国瑞数码零点实验室、河南信安世纪科技有限公司、北京云科安信科技有限公司（Seraph 安全实验室）、新疆海狼科技有限公司、杭州迪普科技股份有限公司、广州市蓝爵计算机科技有限公司、南京众智维信息科技有限公司、山东正中信息技术股份有限公司、江苏保旺达软件技术有限公司、北京山石网科信息技术有限公司、内蒙古奥创科技有限公司、平安银河实验室、北京零零信安科技有限公司、上海观安信息技术股份有限公司、深圳市魔方安全科技有限公司、国家互联网应急中心、北京信联科汇科技有限公司、山东道普测评技术有限公司、山石网科通信技术股份有限公司、四川哨兵信息科技有限公司、西安交大捷普网络科技有限公司、信联科技（南京）有限公司、北京机沃科技有限公司、北京智游网安科技有限公司、广州安亿信软件科技有限公司、京东云安全及其他个人白帽子向 CNVD 提交了 6960 个以事件型漏洞为主的原创漏洞，其中包括斗象科技（漏洞盒子）、上海交大和奇安信网神（补天平台）向 CNVD 共享的白帽子报送的 5569 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） | 2548 | 2548 |
| 斗象科技（漏洞盒子） | 2373 | 2373 |
| 上海交大 | 648 | 648 |
| 哈尔滨安天科技集团股份有限公司 | 242 | 0 |
| 北京天融信网络安全技术有限公司 | 219 | 10 |
| 北京神州绿盟科技有限公司 | 169 | 1 |
| 深信服科技股份有限公司 | 95 | 0 |
| 新华三技术有限公司 | 86 | 0 |
| 华为技术有限公司 | 81 | 0 |
| 中国电信集团系统集成有限责任公司 | 80 | 80 |

| | | |
|---|---|---|
| 厦门服云信息科技有限公司 | 77 | 0 |
| 北京启明星辰信息安全技术有限公司 | 53 | 6 |
| 北京数字观星科技有限公司 | 50 | 0 |
| 中国电信股份有限公司网络安全产品运营中心 | 20 | 0 |
| 北京知道创宇信息技术股份有限公司 | 6 | 5 |
| 山东新潮信息技术有限公司 | 51 | 51 |
| 山东云天安全技术有限公司 | 50 | 50 |
| 远江盛邦（北京）网络安全科技股份有限公司 | 37 | 37 |
| 北京天地和兴科技有限公司 | 34 | 34 |
| 河南灵创电子科技有限公司 | 32 | 32 |
| 国瑞数码零点实验室 | 31 | 31 |
| 河南信安世纪科技有限公司 | 19 | 19 |
| 北京云科安信科技有限公司（Seraph 安全实验室） | 18 | 18 |
| 新疆海狼科技有限公司 | 17 | 17 |
| 杭州迪普科技股份有限公司 | 14 | 0 |
| 广州市蓝爵计算机科技有限公司 | 12 | 12 |
| 南京众智维信息科技有限公司 | 12 | 12 |
| 山东正中信息技术股份有限公司 | 12 | 12 |
| 江苏保旺达软件技术有限公司 | 9 | 9 |
| 北京山石网科信息技术有限公司 | 8 | 8 |
| 内蒙古奥创科技有限公司 | 7 | 7 |
| 平安银河实验室 | 6 | 6 |

| | | |
|---|---|---|
| 北京零零信安科技有限公司 | 5 | 5 |
| 上海观安信息技术股份有限公司 | 4 | 4 |
| 深圳市魔方安全科技有限公司 | 4 | 4 |
| 国家互联网应急中心 | 4 | 4 |
| 北京信联科汇科技有限公司 | 3 | 3 |
| 山东道普测评技术有限公司 | 3 | 3 |
| 山石网科通信技术股份有限公司 | 3 | 3 |
| 四川哨兵信息科技有限公司 | 3 | 3 |
| 西安交大捷普网络科技有限公司 | 3 | 3 |
| 信联科技（南京）有限公司 | 3 | 3 |
| 北京机沃科技有限公司 | 1 | 1 |
| 北京智游网安科技有限公司 | 1 | 1 |
| 广州安亿信软件科技有限公司 | 1 | 1 |
| 京东云安全 | 1 | 1 |
| CNCERT 青海分中心 | 1 | 1 |
| CNCERT 山东分中心 | 1 | 1 |
| 个人 | 893 | 893 |
| 报送总计 | 8050 | 6960 |

## 本周漏洞按类型和厂商统计

本周，CNVD 收录了 266 个漏洞。应用程序 127 个，WEB 应用 84 个，网络设备（交换机、路由器等网络端设备）21 个，操作系统 20 个，智能设备（物联网终端设备）8 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 | 127 |
| WEB 应用 | 84 |
| 网络设备（交换机、路由器等网络端设备） | 21 |
| 操作系统 | 20 |
| 智能设备（物联网终端设备） | 8 |
| 数据库 | 4 |
| 安全产品 | 2 |

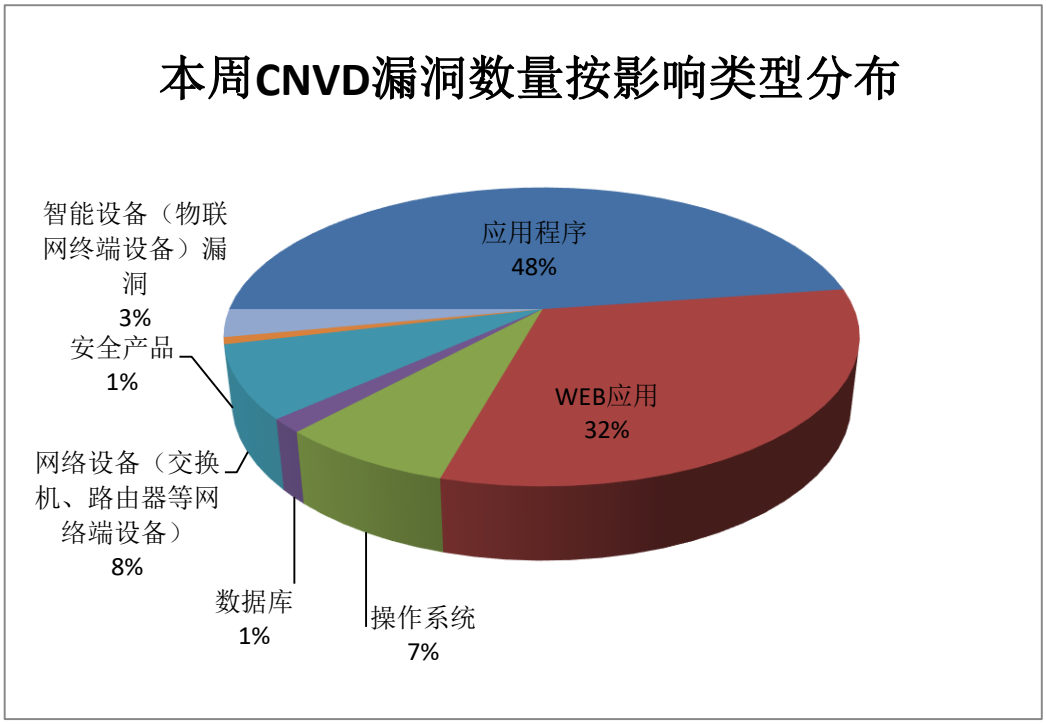


图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Hancom、Microsoft、Intel 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 | Hancom | 40 | 15% |
| 2 | Microsoft | 18 | 7% |
| 3 | Intel | 15 | 6% |
| 4 | IBM | 12 | 5% |
| 5 | Google | 9 | 3% |
| 6 | Apple | 8 | 3% |
| 7 | 广州市花都区新华伟创广告设计服务部 | 6 | 2% |

| | | | |
|---|---|---|---|
| 8 | 深圳市乔安科技有限公司 | 6 | 2% |
| 9 | AikCms | 5 | 2% |
| 10 | 其他 | 147 | 55% |

## 本周行业漏洞收录情况

本周，CNVD 收录了 5 个电信行业漏洞，15 个移动互联网行业漏洞，8 个工控行业漏洞（如下图所示）。其中，“Google Android 缓冲区溢出漏洞（CNVD-2020-68856）、Google Android 缓冲区溢出漏洞（CNVD-2020-68857）”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/

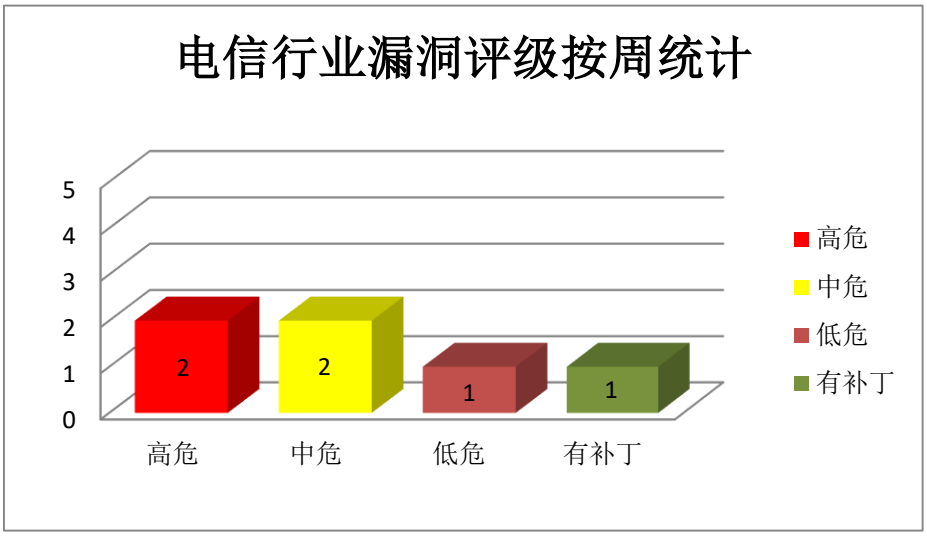


图 3 电信行业漏洞统计

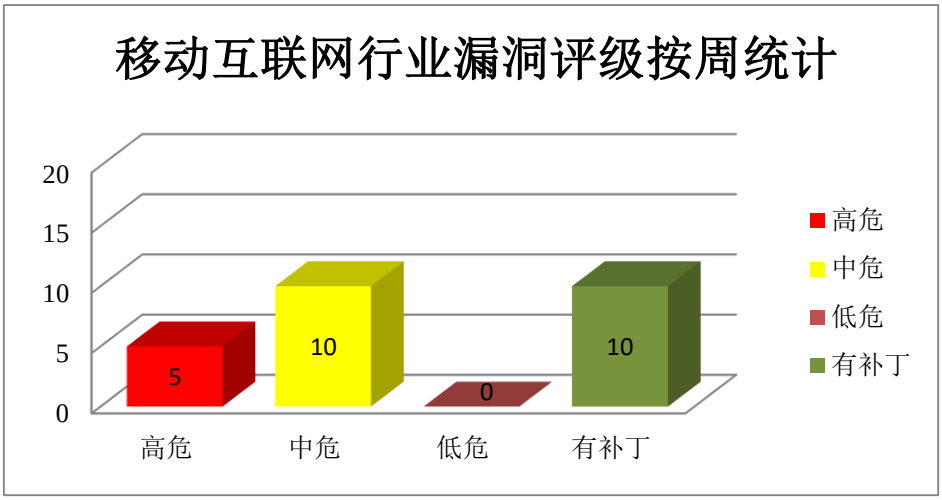


图 4 移动互联网行业漏洞统计

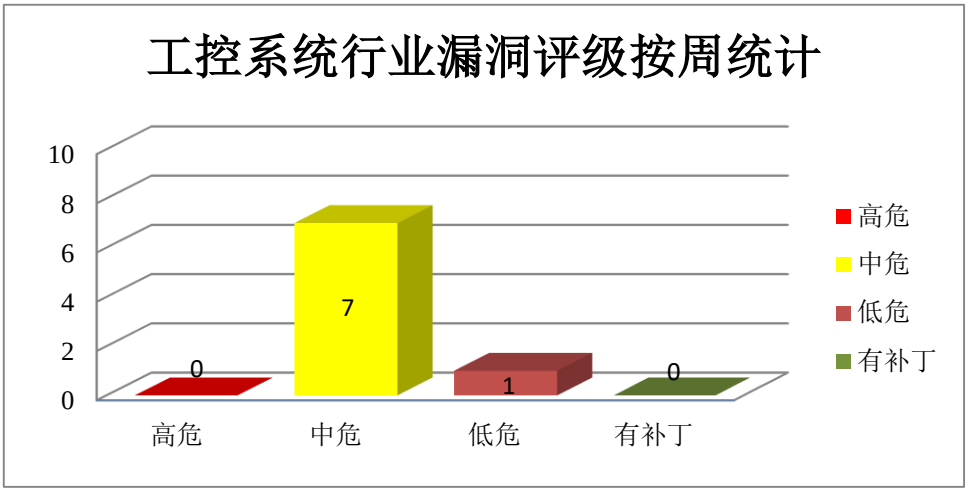


图 5 工控系统行业漏洞统计

## 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、IBM 产品安全漏洞

IBM Spectrum Protect Plus 是用于虚拟环境的数据保护和可用性解决方案。IBM Spectrum Protect Operations Center 是美国 IBM 公司的一个为 IBM Spectrum Protect 环境提供可视化控制的软件。IBM Sterling B2B Integrator 是一个交易引擎，是一套根据您的业务需求运行您定义和管理的流程的组件。IBM Cloud Pak for Security 是一款使用统一接口的集成安全工具，可深入洞察混合多云环境中的威胁。Maxmind Libmaxminddb 是美国 Maxmind 公司的一个用于处理 Maxmind 类型文件的 C 代码库。IBM Cognos Controller 是美国 IBM 公司的一套商业智能与计划解决方案。IBM DB2 是美国 IBM 公司的一套关系型数据库管理系统。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密码、加密密钥等硬编码凭据，创建一个恶意的 DLL，然后将其放到 IBM DB2 的当前目录中，以便执行代码等。

CNVD 收录的相关漏洞包括：IBM Spectrum Protect Plus 硬编码凭据漏洞、IBM Spectrum Protect Operations Center 信息泄露漏洞（CNVD-2020-67638）、IBM Sterling B2B Integrator Standard Edition 弱加密算法漏洞、IBM Cloud Pak for Security 信息泄露漏洞（CNVD-2020-68252）、IBM Cloud Pak for Security 弱加密算法漏洞、Maxmind Libmaxminddb 缓冲区溢出漏洞、IBM Cognos Controller 权限提升漏洞、IBM DB2 任意代码执行漏洞。其中，“IBM Spectrum Protect Plus 硬编码凭据漏洞、IBM DB2 任意代码执行漏洞”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：https://www.cnvd.org.cn/flaw/show/CNVD-2020-67637

https://www.cnvd.org.cn/flaw/show/CNVD-2020-67638

https://www.cnvd.org.cn/flaw/show/CNVD-2020-67834

https://www.cnvd.org.cn/flaw/show/CNVD-2020-68252

https://www.cnvd.org.cn/flaw/show/CNVD-2020-68251

https://www.cnvd.org.cn/flaw/show/CNVD-2020-68258

https://www.cnvd.org.cn/flaw/show/CNVD-2020-68257

https://www.cnvd.org.cn/flaw/show/CNVD-2020-68350

## 2、Microsoft 产品安全漏洞

Microsoft Network Watcher Agent virtual machine extension for Linux 是美国微软（Microsoft）公司的一款 Linux 的虚拟机网络监控插件。Microsoft Visual Studio Code 是美国微软（Microsoft）公司的一款开源的代码编辑器。Microsoft Windows rdp 是美国微软（Microsoft）公司的一款用于连接远程 Windows 桌面的应用。Microsoft Windows 是美国微软（Microsoft）公司的一种桌面操作系统。Microsoft Excel 是美国微软（Microsoft）公司的一款 Office 套件中的电子表格处理软件。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞使用提升的特权执行代码，导致目标系统上的 RDP 服务停止响应等。

CNVD 收录的相关漏洞包括：Microsoft Network Watcher Agent virtual machine extension for Linux 访问控制错误漏洞、Microsoft Visual Studio Code 远程代码执行漏洞、Microsoft Windows rdp 拒绝服务漏洞、Microsoft Windows 内核权限提升漏洞、Microsoft Windows 远程桌面服务拒绝服务漏洞、Microsoft Excel 远程代码执行漏洞（CNVD-2020-68843、CNVD-2020-68842、CNVD-2020-68841）。其中，除“Microsoft Excel 远程代码执行漏洞（CNVD-2020-68843、CNVD-2020-68842、CNVD-2020-68841）”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：https://www.cnvd.org.cn/flaw/show/CNVD-2020-68540

https://www.cnvd.org.cn/flaw/show/CNVD-2020-68539

https://www.cnvd.org.cn/flaw/show/CNVD-2020-68847

https://www.cnvd.org.cn/flaw/show/CNVD-2020-68845

https://www.cnvd.org.cn/flaw/show/CNVD-2020-68848

https://www.cnvd.org.cn/flaw/show/CNVD-2020-68843

https://www.cnvd.org.cn/flaw/show/CNVD-2020-68842

https://www.cnvd.org.cn/flaw/show/CNVD-2020-68841

## 3、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。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。Google Go Cmd/go 是美国谷歌（Google）公司的一个为 Go 语

言提供命令支持的代码库。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-2020-68850、CNVD-2020-68851）、Google Chrome 释放后重用漏洞（CNVD-2020-68853、CNVD-2020-68852）、Google Android 缓冲区溢出漏洞（CNVD-2020-68856、CNVD-2020-68857）、Google Android 权限提升漏洞（CNVD-2020-68855）、Google Go Cmd/go 代码执行漏洞。其中，“Google Android 缓冲区溢出漏洞（CNVD-2020-68856、CNVD-2020-68857）”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-2020-68850

https://www.cnvd.org.cn/flaw/show/CNVD-2020-68853

https://www.cnvd.org.cn/flaw/show/CNVD-2020-68852

https://www.cnvd.org.cn/flaw/show/CNVD-2020-68851

https://www.cnvd.org.cn/flaw/show/CNVD-2020-68856

https://www.cnvd.org.cn/flaw/show/CNVD-2020-68855

https://www.cnvd.org.cn/flaw/show/CNVD-2020-68854

https://www.cnvd.org.cn/flaw/show/CNVD-2020-68857

**4、Intel 产品安全漏洞**

Intel Thunderbolt DCH drivers 是美国因特尔（Intel）公司的一个用于 Windows 的驱动程序。Intel Quartus Prime Pro 是美国英特尔（Intel）公司的一套多平台设计环境。Intel Active Management Technology（AMT）是美国英特尔（Intel）公司的一套以硬件为基础的计算机远程主动管理技术软件。Intel Core Processors 是美国英特尔（Intel）公司的一款 Intel Core 系列中央处理器（CPU）。Intel Microprocessors 是美国英特尔（Intel）公司的微处理器（CPU）产品。Intel Server Board 是美国英特尔（Intel）公司的一款服务器主板。Intel Power Management Controller（Intel PMC）是美国英特尔（Intel）公司的一个用于电源控制的内置程序。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞通过本地访问提升权限，潜在地通过本地访问启用特权升级等。

CNVD 收录的相关漏洞包括：Intel Thunderbolt DCH drivers 权限提升漏洞、Intel Thunderbolt DCH drivers 缓冲区溢出漏洞、Intel Quartus Prime Pro 缓冲区溢出漏洞、Intel AMT 和 Intel ISM 缓冲区溢出漏洞、Intel CSME 权限提升漏洞、Intel(R) Processors 权限提升漏洞、Intel(R) Server Board 权限提升漏洞、Intel(R) Processors PMC 权限提升漏洞。上述漏洞的综合评级为“中危”。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-2020-67833

https://www.cnvd.org.cn/flaw/show/CNVD-2020-67832

https://www.cnvd.org.cn/flaw/show/CNVD-2020-68832

https://www.cnvd.org.cn/flaw/show/CNVD-2020-68831

https://www.cnvd.org.cn/flaw/show/CNVD-2020-68830

https://www.cnvd.org.cn/flaw/show/CNVD-2020-68835

https://www.cnvd.org.cn/flaw/show/CNVD-2020-68834

https://www.cnvd.org.cn/flaw/show/CNVD-2020-68833

**5、PbootCMS 跨站请求伪造漏洞（CNVD-2020-68549）**

PbootCMS 是翱云科技开发的一款全新内核的开源企业建站系统。PbootCMS 1.3.2 存在跨站请求伪造漏洞。攻击者可利用该漏洞更改用户密码。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/show/CNVD-2020-68549

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-2020-67605 | Apple 多款产品缓冲区溢出漏洞（CNVD-2020-67605） | 高 | 厂商已发布了漏洞修复程序，请及时关注更新：https://support.apple.com/en-us/HT210724 |
| CNVD-2020-67604 | News Script PHP Pro 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://simplephpscripts.com/news-script-php-pro/ |
| CNVD-2020-67609 | Apple 多款产品输入验证错误漏洞 | 高 | 目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://support.apple.com/en-us/HT209602 |
| CNVD-2020-67835 | Trend Micro InterScan Web Security Virtual Appliance 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://success.trendmicro.com/solution/000281954 |
| CNVD-2020-68544 | Synology SafeAccess 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://www.synology.com/en-global/security/advisory/Synology_SA_20_25 |
| CNVD-2020-68550 | Huawei FusionCompute 权限提升漏洞 | 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/en/psirt/security-advisories/huawei-sa-20201118-01-pr |

| | | | |
|---|---|---|---|
| | | | ivilege-en |
| CNVD-2020-68860 | FreeBSD 拒绝服务漏洞（CNVD-2020-68860） | 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.freebsd.org/security/advisories/FreeBSD-SA-20:32.rtsold.asc |
| CNVD-2020-68858 | Mozilla Thunderbird 缓冲区溢出漏洞（CNVD-2020-68858） | 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/mfsa2020-53/#CVE-2020-26970 |
| CNVD-2020-68864 | Victor CMS SQL 注入漏洞（CNVD-2020-68864） | 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/BigTiger2020/Victor-CMS-/blob/main/README.md |
| CNVD-2020-68867 | ZXELINK ZXV10 W908 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：http://www.zxelink.com.cn/website/html/CommonContent.html?classify=news&id=43&menuID=20201126153313319 |

小结：本周，IBM 产品被披露存在多个漏洞，攻击者可利用漏洞获取密码、加密密钥等硬编码凭据，创建一个恶意的 DLL，然后将其放到 IBM DB2 的当前目录中，以便执行代码等。此外，Microsoft、Google、Intel 等多款产品被披露存在多个漏洞，攻击者可利用漏洞使用提升的特权执行代码，导致应用程序崩溃，通过本地访问提升权限，潜在地通过本地访问启用特权升级等。另外，PbootCMS 被披露存在跨站请求伪造漏洞。远程攻击者可利用该漏洞更改用户密码。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、Desdev DedeCMS 跨站脚本漏洞

**验证描述**

Desdev DedeCMS（织梦内容管理系统）是中国卓卓网络（Desdev）公司的一套基于 PHP 的开源内容管理系统（CMS）。该系统具有内容发布、内容管理、内容编辑和内容检索等功能。

DedeCMS 5.8 版本存在跨站脚本漏洞，该漏洞源于允许恶意用户向 web 页面注入代码，其他用户在浏览 web 页面时会受到影响。目前没有详细的漏洞细节提供。

**验证信息**

POC 链接：https://www.exploit-db.com/exploits/48974

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2020-68837

**信息提供者**

新华三技术有限公司

*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. 工信部通报 60 家侵害用户权益行为 App：嗨玩、高铁管家等上榜

截至目前，尚有 60 款 App 未完成整改（详见附件），上述 App 应在 12 月 10 日前完成整改落实工作。逾期不整改的，我部将依法依规组织开展相关处置工作。

参考链接：https://www.cnbeta.com/articles/tech/1061417.htm

### 2. Google 开发者披露 iPhone Wi-Fi 漏洞发现过程

今年早些时候，苹果修复了 iPhone 的一个高危漏洞，该漏洞是 iOS 内核内存破坏 bug 导致的，允许攻击者通过 Wi-Fi 远程访问整个设备，整个过程无需任何用户交互。Google Project Zero 安全研究员 Ian Beer 向苹果报告了该漏洞并开发出了漏洞利用的 POC。他在官方博客上详细讲述了 Wi-Fi 漏洞的发现过程。

参考链接：https://www.solidot.org/story?sid=66258

### 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