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 23 日-2020 年 11 月 29 日　　2020 年第 48 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 360 个，其中高危漏洞 89 个、中危漏洞 200 个、低危漏洞 71 个。漏洞平均分值为 5.79。本周收录的漏洞中，涉及 0day 漏洞 126 个（占 35%），其中互联网上出现“SourceCodester Gym Management System 跨站脚本漏洞、WordPress Fancy Product Designer For WooCommerce 文件上传漏洞”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 4662 个，与上周（4995 个）环比减少 7%。

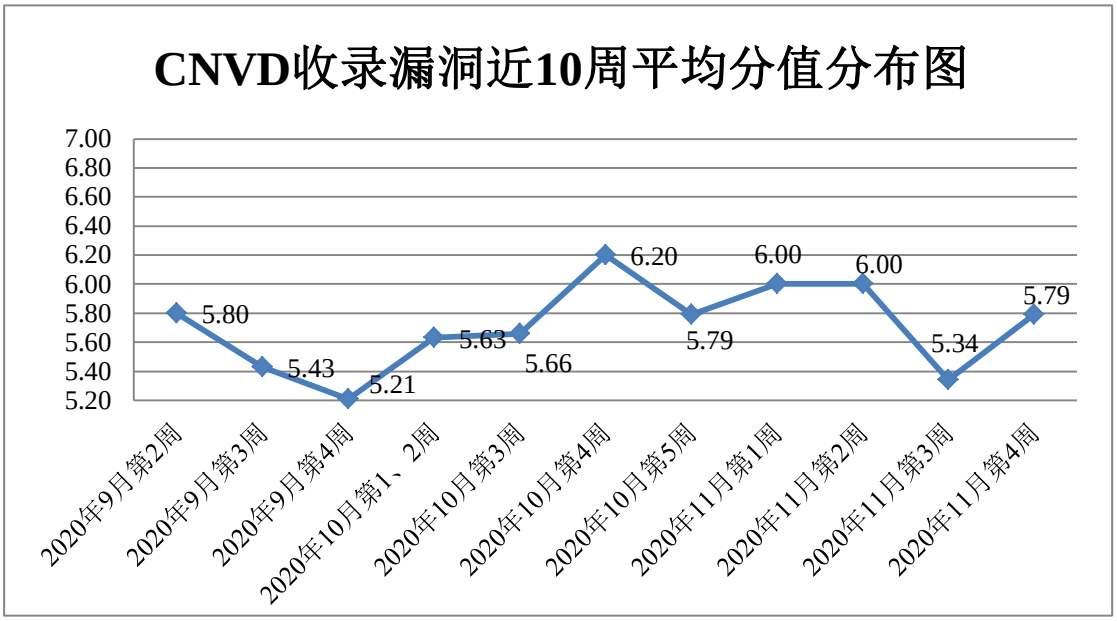

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 26 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 473 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 38 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 39 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：

上海步科自动化股份有限公司、深圳市圆梦云科技有限公司、北京指掌易科技有限公司、厦门网中网软件有限公司、北京通达信科科技有限公司、深圳市乔安科技有限公司、青岛易企天创管理咨询有限公司、河南青否网络科技有限公司、江苏宿迁金典科技有限公司、上海浪擎信息科技有限公司、石家庄瑞诺网络科技有限公司、金蝶软件（中国）有限公司、睿谷信息科技有限公司、用友网络科技股份有限公司、浙江浙大中控信息技术有限公司、天津南大通用数据技术股份有限公司、成都依能科技股份有限公司、深圳市藏海科技有限公司、昆明云涛科技有限公司、盐城腾飞网络科技有限公司、杭州麦达电子有限公司、廊坊市极致网络科技有限公司、戴尔(中国)有限公司、烟台艾睿光电科技有限公司、上海李宁体育用品电子商务有限公司、居易科技股份有限公司、北京网御星云信息技术有限公司、北京国炬信息技术有限公司、广州热点软件科技股份有限公司、厦门四信通信科技有限公司、广东凯格科技有限公司、中国中铁置业集团、海洋 CMS、爱客 CMS、狂雨小说 cms、KKCMS、SEMCMS、HadSky、ucms、NETGEAR 和 yycms。

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、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、中国电信集团系统集成有限责任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、北京山石网科信息技术有限公司、河南信安世纪科技有限公司、西安交大捷普网络科技有限公司、山东云天安全技术有限公司、河南灵创电子科技有限公司、北京天地和兴科技有限公司、内蒙古奥创科技有限公司、北京顶象技术有限公司、山东华鲁科技发展股份有限公司、北京安华金和科技有限公司、远江盛邦（北京）网络安全科技股份有限公司、山东正中信息技术股份有限公司、广州市蓝爵计算机科技有限公司、北京云科安信科技有限公司（Seraph 安全实验室）、上海观安信息技术股份有限公司、南京众智维信息科技有限公司、北京零零信安科技有限公司、吉林谛听信息技术有限公司、北京机沃科技有限公司、中移（杭州）信息技术有限公司、上海纽盾科技股份有限公司、四川哨兵信息科技有限公司、深圳市魔方安全科技有限公司、北京华云安信息技术有限公司、广东励勤信息技术有限公司、北京智游网安科技有限公司、山石网科通信技术股份有限公司及其他个人白帽子向 CNVD 提交了 4662 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 2598 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）	1801	1801
上海交大	559	559
北京天融信网络安全技术有限公司	465	8
北京神州绿盟科技有限公司	319	7
奇安信网神（补天平台）	238	238
哈尔滨安天科技集团股份有限公司	225	0
深信服科技股份有限公司	131	0
中国电信集团系统集成有限责任公司	106	106
北京奇虎科技有限公司	91	0
新华三技术有限公司	82	0
华为技术有限公司	70	0
北京启明星辰信息安全技术有限公司	60	2
北京数字观星科技有限公司	48	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	1
腾讯安全云鼎实验室	2	0
国瑞数码零点实验室	197	197
北京华顺信安科技有限公司	99	0
山东新潮信息技术有限公司	78	78

北京山石网科信息技术有限公司	56	56
河南信安世纪科技有限公司	41	41
西安交大捷普网络科技有限公司	37	37
山东云天安全技术有限公司	33	33
河南灵创电子科技有限公司	28	28
北京天地和兴科技有限公司	21	21
内蒙古奥创科技有限公司	17	17
北京顶象技术有限公司	15	15
山东华鲁科技发展股份有限公司	15	15
杭州迪普科技股份有限公司	15	0
北京安华金和科技有限公司	8	8
远江盛邦（北京）网络安全科技股份有限公司	8	8
山东正中信息技术股份有限公司	7	7
广州市蓝爵计算机科技有限公司	6	6
北京云科安信科技有限公司（Seraph 安全实验室）	6	6
上海观安信息技术股份有限公司	4	4
南京众智维信息科技有限公司	4	4
北京零零信安科技有限公司	3	3
吉林谛听信息技术有限公司	3	3
北京机沃科技有限公司	3	3
中移（杭州）信息技术有限公司	2	2
上海纽盾科技股份有限公司	2	2

四川哨兵信息科技有限公司	1	1
深圳市魔方安全科技有限公司	1	1
北京华云安信息技术有限公司	1	1
广东励勤信息技术有限公司	1	1
北京智游网安科技有限公司	1	1
山石网科通信技术股份有限公司	1	1
CNCERT 辽宁分中心	17	17
CNCERT 贵州分中心	4	4
CNCERT 青海分中心	4	4
CNCERT 海南分中心	2	2
CNCERT 甘肃分中心	2	2
CNCERT 河北分中心	1	1
个人	1310	1310
报送总计	6277	4662

本周漏洞按类型和厂商统计

本周，CNVD 收录了 360 个漏洞。应用程序 155 个，WEB 应用 118 个，操作系统 48 个，网络设备（交换机、路由器等网络端设备）15 个，智能设备（物联网终端设备）12 个，数据库 7 个，安全产品 5 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	155
WEB 应用	118
操作系统	48
网络设备（交换机、路由器等网络端设备）	15
智能设备（物联网终端设备）	12
数据库	7
安全产品	5

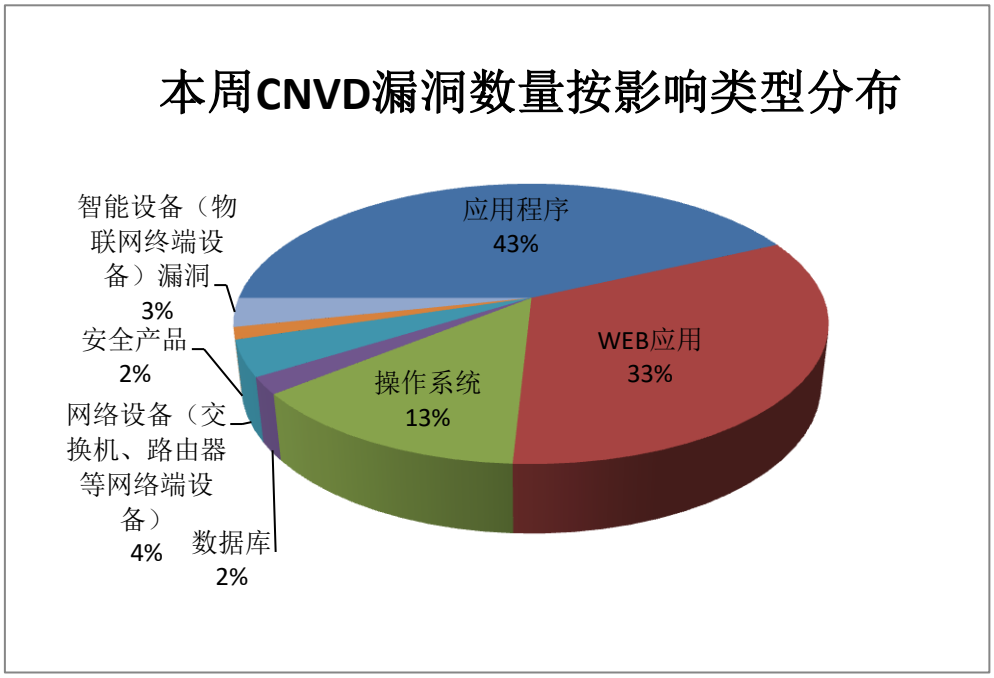

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Apple、SAP、Cisco 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	Apple	37	10%
2	SAP	25	7%
3	Cisco	20	6%
4	Intel	18	5%
5	F5	15	4%
6	Victor CMS	12	3%
7	盾灵科技	12	3%
8	JetBrains	10	3%
9	Samsung	9	3%
10	其他	202	56%

本周行业漏洞收录情况

本周，CNVD 收录了 9 个电信行业漏洞，55 个移动互联网行业漏洞，3 个工控行业漏洞（如下图所示）。其中，“多款 Apple 产品内存初始化漏洞、Google Android 远程代

码执行漏洞（CNVD-2020-65246）、多款 Apple 产品越界读取漏洞（CNVD-2020-65927）”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/

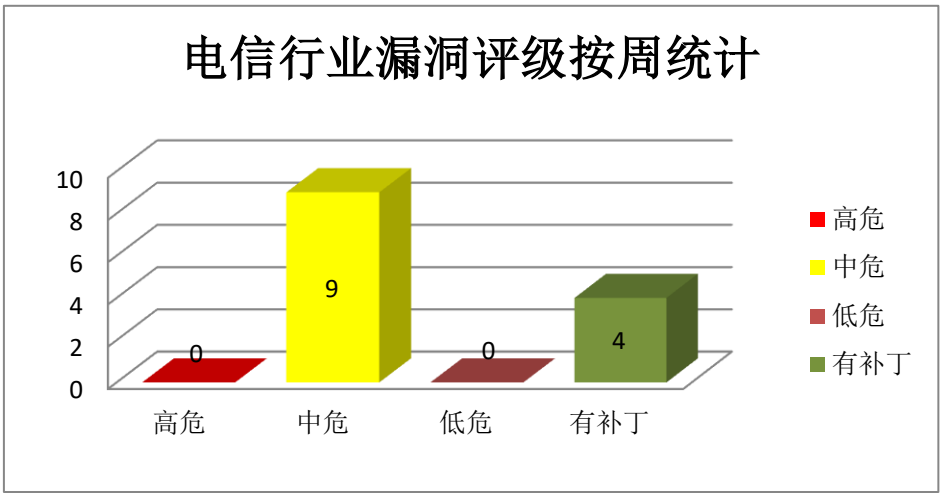

图 3 电信行业漏洞统计

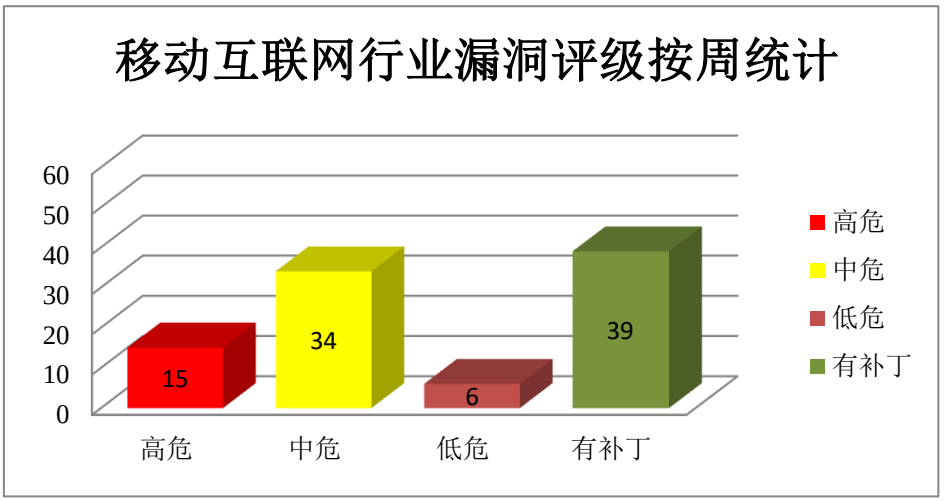

图 4 移动互联网行业漏洞统计

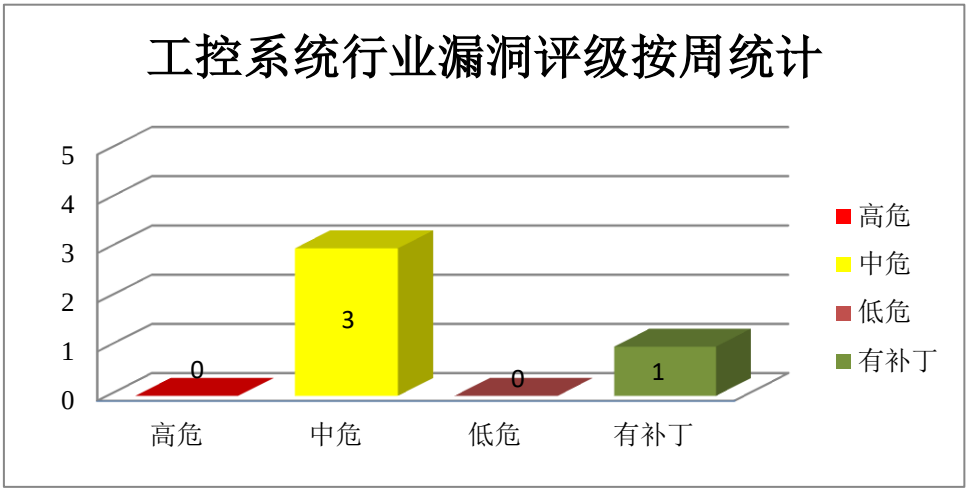

图 5 工控系统行业漏洞统计

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 是一款苹果公司的 Mac 平台上的操作系统。Apple iOS 是一套为移动设备所开发的操作系统。Apple iPadOS 是一套用于 iPad 平板电脑的操作系统。Apple watchOS 是一套智能手表操作系统。Apple tvOS 是一套智能电视操作系统。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞以内核权限执行任意代码等。

CNVD 收录的相关漏洞包括：Apple macOS Catalina 蓝牙内存破坏漏洞、多款 Apple 产品 Kernel 组件内存破坏漏洞（CNVD-2020-65921、CNVD-2020-65922）、多款 Apple 产品 Kernel 组件信息泄露漏洞（CNVD-2020-65923）、多款 Apple 产品越界读取漏洞（CNVD-2020-65927）、多款 Apple 产品 Kernel 组件整数溢出漏洞、多款 Apple 产品内存破坏漏洞（CNVD-2020-65942）、多款 Apple 产品内存初始化漏洞。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-2020-65913

https://www.cnvd.org.cn/flaw/show/CNVD-2020-65921

https://www.cnvd.org.cn/flaw/show/CNVD-2020-65923

https://www.cnvd.org.cn/flaw/show/CNVD-2020-65922

https://www.cnvd.org.cn/flaw/show/CNVD-2020-65927

https://www.cnvd.org.cn/flaw/show/CNVD-2020-65925

https://www.cnvd.org.cn/flaw/show/CNVD-2020-65942

https://www.cnvd.org.cn/flaw/show/CNVD-2020-65941

2、Cisco 产品安全漏洞

Cisco Security Manager（CSM）是一套企业级的管理应用，它主要用于在 Cisco 网络和安全设备上配置防火墙、VPN 和入侵保护安全服务。Cisco DNA Spaces: Connector 用于将 Cisco DNA Spaces 连接到 Cisco 无线控制器。Cisco Integrated Management Controller (IMC)是一个为 Cisco UCS C 系列机架式服务器和 Cisco S 系列存储服务器提供嵌入式服务器管理的基板管理控制器。Cisco IoT Field Network Director (FND)是大规模 FAN 部署的网络管理系统。Cisco Adaptive Security Appliance (ASA)软件是为 Cisco ASA 系列提供核心操作系统。Cisco SD-WAN Solution 是 Cisco 的一套网络扩展解决方案，vManage 是其中的控制台。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞访问后端数据库并读取、更改或删除信息，执行任意命令，导致设备重新加载等。

CNVD 收录的相关漏洞包括：Cisco Security Manager 输入验证错误漏洞、Cisco DNA Spaces Connector 命令注入漏洞、Cisco Integrated Management Controller 远程代码执行漏洞、Cisco IoT Field Network Director SOAP API 授权绕过漏洞、Cisco IoT Field Network Director 权限提升漏洞、Cisco Adaptive Security Appliance (ASA)软件拒绝服务漏洞、Cisco SD-WAN vManage XML 外部实体注入漏洞（CNVD-2020-66212、CNVD-2020-66211）。其中，除“Cisco SD-WAN vManage XML 外部实体注入漏洞（CNVD-2020-66212、CNVD-2020-66211）”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-2020-66202
https://www.cnvd.org.cn/flaw/show/CNVD-2020-66205
https://www.cnvd.org.cn/flaw/show/CNVD-2020-66204
https://www.cnvd.org.cn/flaw/show/CNVD-2020-66208
https://www.cnvd.org.cn/flaw/show/CNVD-2020-66206
https://www.cnvd.org.cn/flaw/show/CNVD-2020-66213
https://www.cnvd.org.cn/flaw/show/CNVD-2020-66212
https://www.cnvd.org.cn/flaw/show/CNVD-2020-66211

3、SAP 产品安全漏洞

SAP Netweaver 是一套面向服务的集成化应用平台。SAP Fiori 是一套为 SAP 应用程序提供用户体验（UX）的设计系统，它为设计人员和开发人员提供了一套工具和指南，能够快速地开发适用于任何平台的应用，为创建者和用户提供一致、创新的体验。SAP Solution Manager 是一套集系统监控、SAP 支持桌面、自助服务、ASAP 实施等多个功能为一体的系统管理平台。SAP 3D Visual Enterprise Viewer 是一款适用于 Windows 的免费 3D 可视化查看器。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，导致应用程序崩溃等。

CNVD 收录的相关漏洞包括：SAP NetWeaver AS ABAP 信息泄露漏洞（CNVD-2020-65554）、SAP Fiori Launchpad 服务器端请求伪造漏洞、SAP Solution Manager 和 SAP Focused Run 操作系统命令注入漏洞、SAP 3D visual Enterprise Viewer 输入验证错误漏洞（CNVD-2020-65565、CNVD-2020-65566、CNVD-2020-65564、CNVD-2020-65567、CNVD-2020-65568）。其中，“SAP Fiori Launchpad 服务器端请求伪造漏洞、SAP Solution Manager 和 SAP Focused Run 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：https://www.cnvd.org.cn/flaw/show/CNVD-2020-65554
https://www.cnvd.org.cn/flaw/show/CNVD-2020-65556
https://www.cnvd.org.cn/flaw/show/CNVD-2020-65563
https://www.cnvd.org.cn/flaw/show/CNVD-2020-65565
https://www.cnvd.org.cn/flaw/show/CNVD-2020-65566
https://www.cnvd.org.cn/flaw/show/CNVD-2020-65564
https://www.cnvd.org.cn/flaw/show/CNVD-2020-65567
https://www.cnvd.org.cn/flaw/show/CNVD-2020-65568

4、Google 产品安全漏洞

Android 是美国 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，提升权限，执行代码，导致拒绝服务。

CNVD 收录的相关漏洞包括：Google Android 远程代码执行漏洞（CNVD-2020-65248、CNVD-2020-65246、CNVD-2020-65249）、Google Android 权限提升漏洞（CNVD-2020-65247、CNVD-2020-65250）、Google Android 信息泄露漏洞（CNVD-2020-65245）、Google Android 拒绝服务漏洞（CNVD-2020-65251、CNVD-2020-65252）。其中，“Google Android 远程代码执行漏洞（CNVD-2020-65246、CNVD-2020-65249）、Google Android 拒绝服务漏洞（CNVD-2020-65251、CNVD-2020-65252）”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-2020-65248
https://www.cnvd.org.cn/flaw/show/CNVD-2020-65247
https://www.cnvd.org.cn/flaw/show/CNVD-2020-65246
https://www.cnvd.org.cn/flaw/show/CNVD-2020-65245
https://www.cnvd.org.cn/flaw/show/CNVD-2020-65251
https://www.cnvd.org.cn/flaw/show/CNVD-2020-65250
https://www.cnvd.org.cn/flaw/show/CNVD-2020-65249

https://www.cnvd.org.cn/flaw/show/CNVD-2020-65252

5、Paradox IP150 缓冲区溢出漏洞

Paradox IP150 是一个提供通过网络来监控管理 Paradox 设备的通信模块。本周，Paradox IP150 被披露存在缓冲区溢出漏洞。远程攻击者可利用该漏洞提交特殊的请求，可以应用程序上下文执行任意代码或使应用程序崩溃。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-2020-66574

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-2020-65243	Azure Sphere 权限提升漏洞（CNVD-2020-65243）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2020-16989
CNVD-2020-65902	Microsoft Azure Sphere 未签名代码执行漏洞（CNVD-2020-65902）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2020-16982
CNVD-2020-65935	Apple macOS Mojave 内存破坏漏洞	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/HT209139
CNVD-2020-66309	HCL Domino 拒绝服务漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0085303&sys_kb_id=2e41878edba0e854a45ad9fcd3961974
CNVD-2020-66577	IBM DB2 缓冲区溢出漏洞（CNVD-2020-66577）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.ibm.com/support/pages/node/6369607
CNVD-2020-66586	Qualcomm MHI Ring Validation 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://www.qualcomm.com/company/product-security/bulletins/november-2020-security-bulletin
CNVD-2020-66592	Intel Open WebRTC Toolkit 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.intel.com/content/www/us/en/security-center/advisory/intel-sa-00424.html
CNVD-2020-66600	Tobesoft Xplatform 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://www.boho.or.kr/krcert/secNoticeView.do?bulletin_writing_sequence=35789
CNVD-2020-66861	Apache Airflow 未授权访问漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://lists.apache.org/thread.html/r23a81b247aa346ff193670be565b2b8ea4b17ddbc7a35fc099c1aadd%40%3Cdev.airflow.apache.org%3E
CNVD-2020-67085	Atlassian Fisheye Crucible 拒绝服务漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.atlassian.com/zh/software/fisheye

小结：本周，Apple 产品被披露存在多个漏洞，攻击者可利用漏洞以内核权限执行任意代码等。此外，Cisco、SAP、Google 等多款产品被披露存在多个漏洞，攻击者可利用漏洞访问后端数据库并读取、更改或删除信息，提升权限，执行任意命令，导致拒绝服务等。另外，Paradox IP150 被披露存在缓冲区溢出漏洞。远程攻击者可利用该漏洞提交特殊的请求，可以应用程序上下文执行任意代码或使应用程序崩溃。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、WordPress Fancy Product Designer For WooCommerce 文件上传漏洞

验证描述

WordPress 是 WordPress 基金会的一套使用 PHP 语言开发的博客平台。该平台支持在 PHP 和 MySQL 的服务器上架设个人博客网站。

WordPress Fancy Product Designer For WooCommerce 存在文件上传漏洞，攻击者可利用漏洞获得服务器权限。

验证信息

POC 链接：https://packetstormsecurity.com/files/160121/WordPress-Fancy-Product-Designer-For-WooCommerce-4.5.1-File-Upload.html

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2020-67562

信息提供者

深信服科技股份有限公司

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. 0patch 发布免费补丁：修复 Windows 7 中的本地提权漏洞

Windows 7 尽管已经停止支持，但全球依然有数百万人在使用它。本月初，一位安全研究人员在 Windows 7 和 Windows Server 2008 R2 上发现了本地提权漏洞。虽然尚不清楚微软是否会为付费扩展支持用户提供补丁修复，但肯定的是当前仍在使用 Windows 7 的普通用户依然非常容易受到攻击。

参考链接：https://www.cnbeta.com/articles/tech/1058609.htm

2. 研究人员展示了如何在几分钟内偷走特斯拉 Model X

研究人员通过利用汽车无钥匙进入系统中的漏洞，展示了在几分钟之内窃取特斯拉 ModelX。8 月份研究人员向特斯拉报告了该漏洞，并且汽车制造商通过远程更新（版本 2020.48）解决了这些漏洞，目前该更新正在推广至车辆。

参考链接：https://securityaffairs.co/wordpress/111340/hacking/researchers-show-how-to-steal-a-tesla-model-x-in-a-few-minutes.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