国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2020 年 03 月 09 日-2020 年 03 月 15 日　　2020 年第 11 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 417 个，其中高危漏洞 138 个、中危漏洞 220 个、低危漏洞 59 个。漏洞平均分值为 6.12。本周收录的漏洞中，涉及 0day 漏洞 114 个（占 27%），其中互联网上出现“ACD Systems ACDSee Photo Studio Standard 缓冲区溢出漏洞、Nature Easy Soft Network Technology ZenTao 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 2537 个，与上周（2227 个）环比增加 14%。

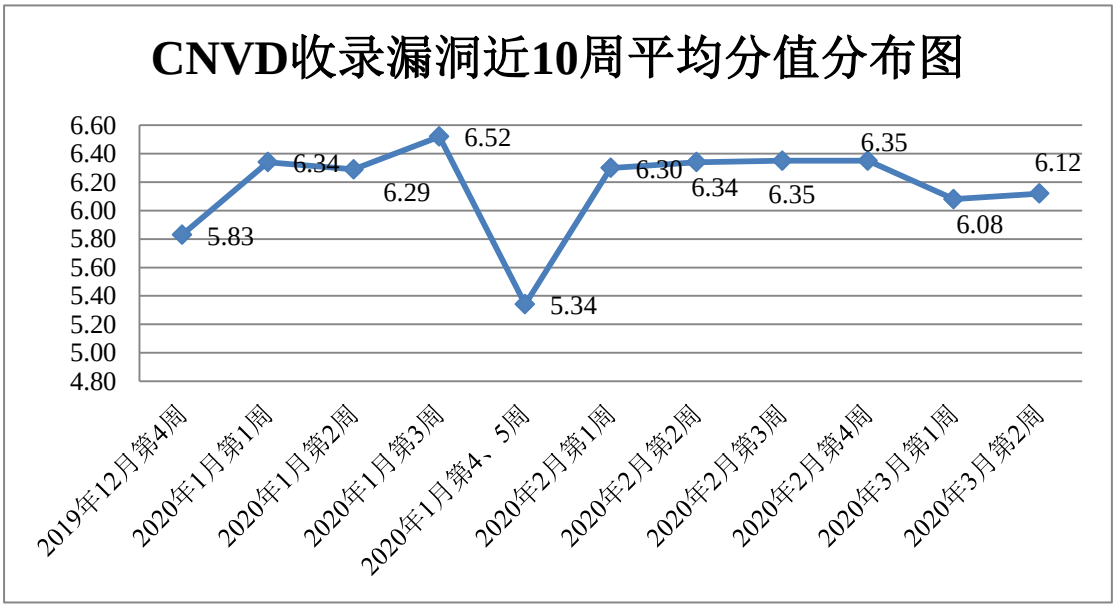

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 61 起，向基础电信企业通报漏洞事件 4 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 345 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 47 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 19 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：

昆明云涛科技有限公司、深圳市迪元素科技有限公司、若无（上海）信息科技有限公司、龙采科技集团有限责任公司、淄博闪灵网络科技有限公司、青岛易软天创网络科技有限公司、上海企炬广告传媒有限公司、湖北淘码千维信息科技有限公司、长沙米拓信息技术有限公司、深圳雅科网络科技有限公司、成都飞鱼星科技股份有限公司、连云港连普信息科技有限公司、福建福昕软件开发股份有限公司、北京圣辉友联网络科技有限公司、桂林佳朋信息科技有限公司、陕西公众软件有限责任公司、四平市九州易通科技有限公司、黄石市科威自控有限公司、翰特网络科技有限公司、成都市灵奇空间软件有限公司、珠海金山软件股份有限公司、海南联拓科技有限公司、苏州科达科技股份有限公司、北京亚控科技发展有限公司、深圳市科脉技术股份有限公司、广西集翔网大信息科技有限公司、深圳市富途网络科技有限公司、广州华多网络科技有限公司、益盟股份有限公司、厦门百胜通软件技术有限公司、北京世纪飞育软件有限责任公司、深圳市驱动人生科技股份有限公司、上海互盾信息科技有限公司、秦皇岛市创想信息网络有限公司、深圳市云趣网络科技股份有限公司、深圳市硕赢互动信息技术有限公司、南大傲拓科技江苏股份有限公司、北京搜狗信息服务有限公司、北京网易有道计算机系统有限公司、怀化第五元素网络信息有限公司、深圳市物联锁科技有限公司、广州商淘信息科技有限公司、哈尔滨伟成科技有限公司、佛山市云迈电子商务有限公司、无锡信捷电气股份有限公司、北京海腾时代科技有限公司、上海丹帆网络科技有限公司、济南爱程网络科技有限公司、大庆久久网络科技有限公司、镇江市云优网络科技有限公司、海南易而优科技有限公司、北京因酷时代科技有限公司、广州搜客网络科技有限公司、北京国炬信息技术有限公司、烟台云脉网络科技有限公司、武汉创益云信息技术有限公司、北京智齿博创科技有限公司、北京快手科技有限公司、深圳市博士通科技有限公司、青岛网搜网络技术有限公司、友讯电子设备（上海）有限公司、常州市青之峰网络科技有限公司、明镜远大网络安全信息技术有限公司、漳州豆壳网络科技有限公司、上海秀可视科技有限公司、郑州微口网络科技有限公司、广州市创科网络科技有限公司、锐捷网络股份有限公司、南京友个软件有限公司、保定互动营销、流星网络电视、无忧网络、DM 企业建站系统、海洋 CMS、Catfish(鲶鱼) CMS、Cisco Systems, Inc.、Zzzcms、CLTPHP、115CMS、YIXUNCMS、XYCMS、SchoolCMS、Jpress 和 WMCMS 团队。

本周，CNVD 发布了《Microsoft 发布 2020 年 3 月安全更新》。详情参见 CNVD 网站公告内容。

https://www.cnvd.org.cn/webinfo/show/5443

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、华为技术有限公司、哈尔滨安天科技集团股份有限公司、恒安嘉新(北京)科技股份公司、北京天融信网络安全技术有限公司等单位报送公开收集的漏洞数量较多。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、长春嘉诚信息技术股份有限公司、国瑞数码零点实验室、北京铭图天成信息技术有限公司、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、上海观安信息技术股份有限公司、北京圣博润高新技术股份有限公司、博智安全科技股份有限公司、山东新潮信息技术有限公司、山石网科通信技术股份有限公司、河北昆时网络科技股份有限公司、广西启汇壹星信息科技有限公司、河南信安世纪科技有限公司、济南三泽信息安全测评有限公司、山东云天安全技术有限公司、北京机沃科技有限公司、辽宁北方实验室有限公司、北京智游网安科技有限公司、南瑞集团公司（国网电力科学研究院）、厦门靠谱云股份有限公司、北京天防安全科技有限公司及其他个人白帽子向 CNVD 提交了 2537 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 1839 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）	844	844
斗象科技（漏洞盒子）	690	690
阿里云计算有限公司	538	0
上海交大	305	305
华为技术有限公司	289	0
哈尔滨安天科技集团股份有限公司	201	0
恒安嘉新(北京)科技股份公司	156	0
北京天融信网络安全技术有限公司	153	8
北京神州绿盟科技有限公司	103	8
深信服科技股份有限公司	70	4

北京启明星辰信息安全技术有限公司	66	14
新华三技术有限公司	57	0
北京数字观星科技有限公司	40	0
南京联成科技发展股份有限公司	19	19
北京奇虎科技有限公司	11	0
北京安信天行科技有限公司	5	5
北京知道创宇信息技术股份有限公司	3	0
南京铱迅信息技术股份有限公司	3	3
远江盛邦（北京）网络安全科技股份有限公司	45	45
内蒙古洞明科技有限公司	40	40
长春嘉诚信息技术股份有限公司	40	40
国瑞数码零点实验室	27	27
北京铭图天成信息技术有限公司	26	26
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	14	0
北京华云安信息技术有限公司	10	10
上海观安信息技术股份有限公司	9	9
北京圣博润高新技术股份有限公司	6	6
博智安全科技股份有限公司	5	5
山东新潮信息技术有限公司	5	5
山石网科通信技术股份有限公司	4	4
河北昆时网络科技股份有限公司	3	3

广西启汇壹星信息科技有限公司	2	2
河南信安世纪科技有限公司	2	2
济南三泽信息安全测评有限公司	2	2
山东云天安全技术有限公司	2	2
北京机沃科技有限公司	1	1
辽宁北方实验室有限公司	1	1
北京智游网安科技有限公司	1	1
南瑞集团公司（国网电力科学研究院）	1	1
厦门靠谱云股份有限公司	1	1
北京天防安全科技有限公司	1	1
CNCERT 宁夏分中心	15	15
CNCERT 福建分中心	7	7
CNCERT 吉林分中心	7	7
CNCERT 江西分中心	6	6
CNCERT 天津分中心	6	6
CNCERT 安徽分中心	5	5
CNCERT 河北分中心	5	5
CNCERT 四川分中心	5	5
CNCERT 青海分中心	4	4
CNCERT 广西分中心	2	2
CNCERT 海南分中心	1	1
CNCERT 重庆分中心	1	1
个人	317	317

报送总计	4204	2537

本周漏洞按类型和厂商统计

本周，CNVD 收录了 417 个漏洞。应用程序 224 个，WEB 应用 61 个，操作系统 59 个，网络设备（交换机、路由器等网络端设备）53 个，安全产品 10 个，数据库 5 个，智能设备（物联网终端设备）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	224
WEB 应用	61
操作系统	59
网络设备（交换机、路由器等网络端设备）	53
安全产品	10
数据库	5
智能设备（物联网终端设备）	5

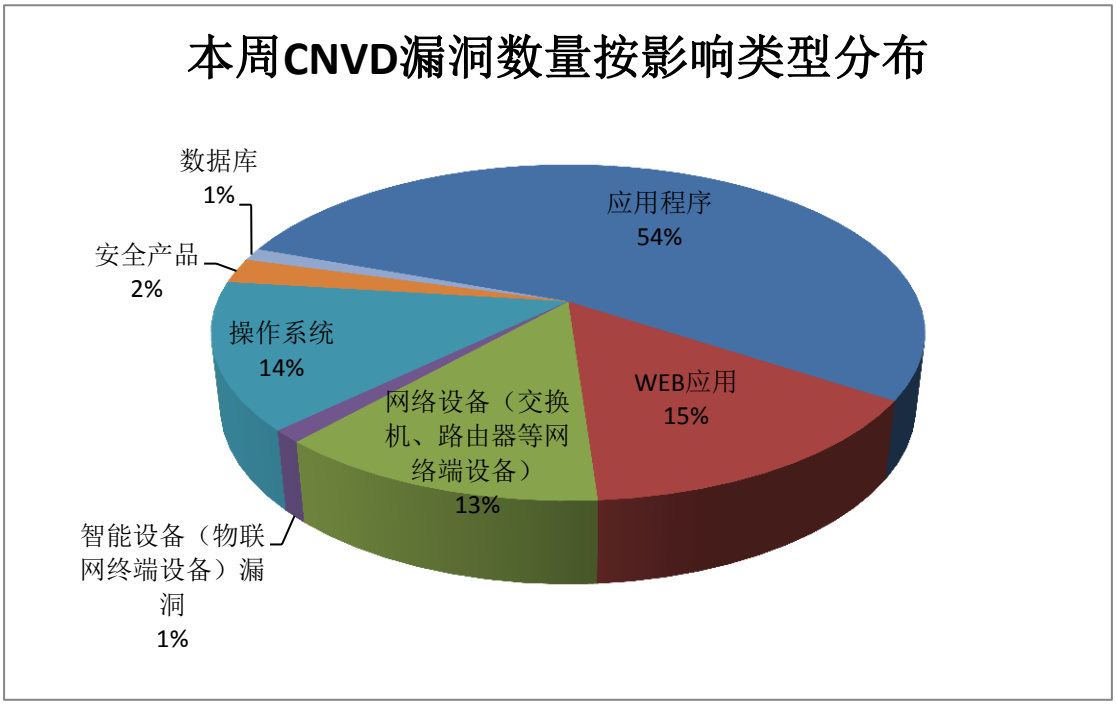

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Microsoft、Google、Chadha 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	Microsoft	38	9%
2	Google	32	8%
3	Chadha	27	6%
4	Qualcomm	20	5%
5	Cisco	19	5%
6	WAGO	18	4%
7	Oracle	16	4%
8	WordPress	14	3%
9	CloudBees	13	3%
10	其他	220	53%

本周行业漏洞收录情况

本周，CNVD 收录了 10 个电信行业漏洞，35 个移动互联网行业漏洞，37 个工控行业漏洞（如下图所示）。其中，“多款 Qualcomm 产品缓冲区溢出漏洞（CNVD-2020-16052）、Google Android System 越界读取漏洞、ABB eSOMS SQL 注入漏洞、Cisco Nexus 9000 Series Fabric Switches 缓冲区溢出漏洞、Google Android Framework 竞争条件问题漏洞”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/

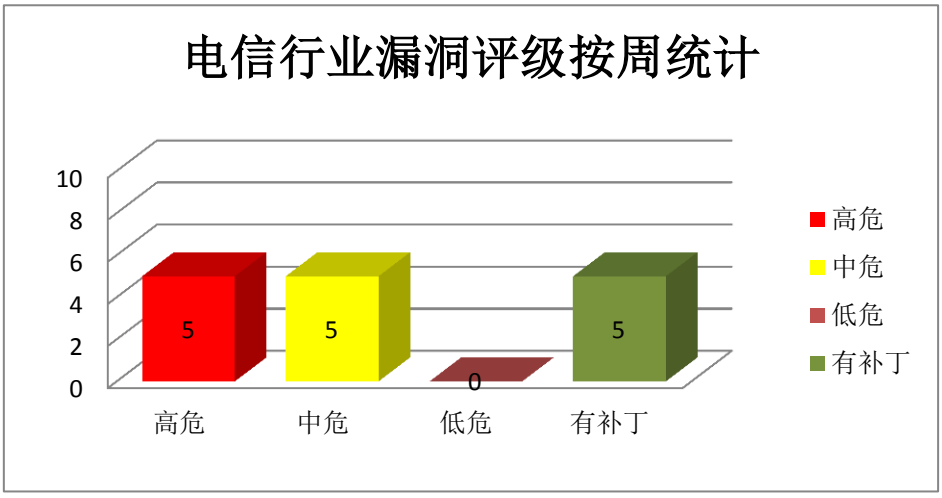

图 3 电信行业漏洞统计

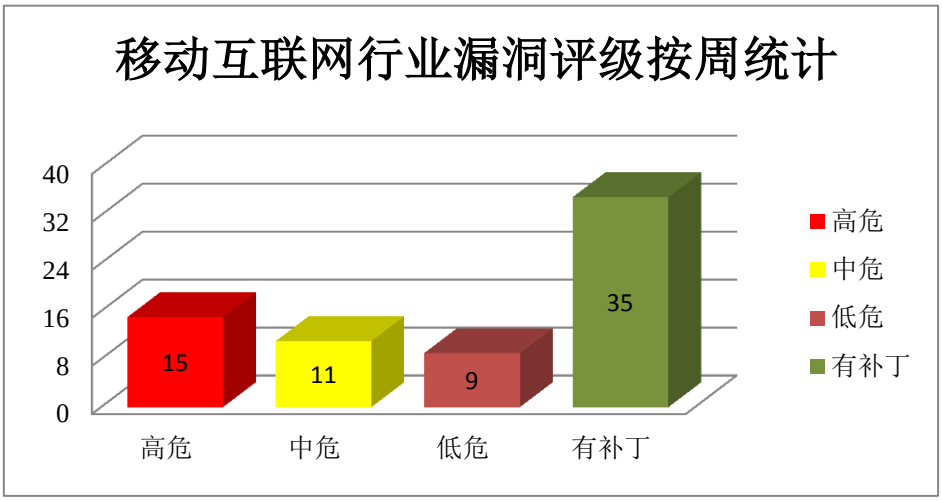

图 4 移动互联网行业漏洞统计

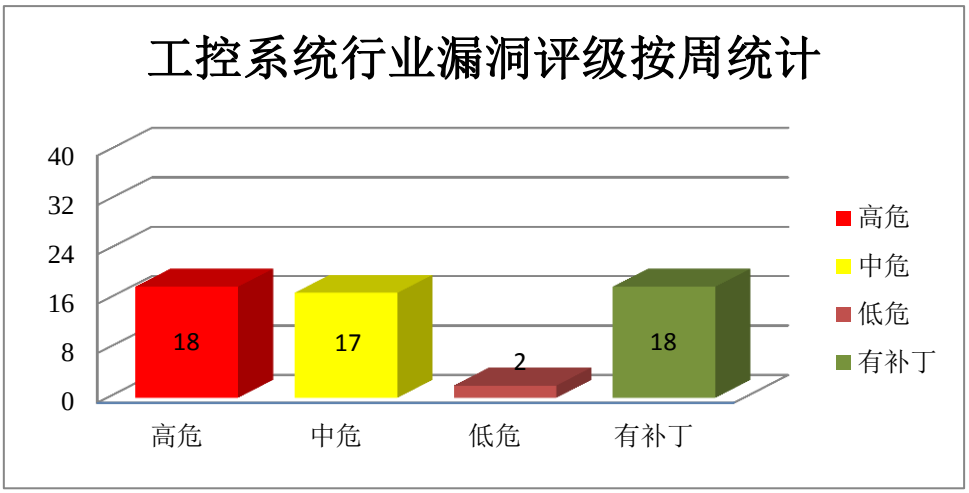

图 5 工控系统行业漏洞统计

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、Microsoft 产品安全漏洞

Microsoft Windows Remote Desktop Gateway 是一款基于 Windows 的远程桌面网关。Microsoft ASP.NET Core 是一框跨平台开源框架。Microsoft Remote Desktop Client 是一款远程桌面客户端。Microsoft Word 是一套 Office 套件中的文字处理软件。Microsoft Dynamics Business Central 是一套企业资源计划系统。Microsoft Windows 是一套个人设备使用的操作系统。Microsoft Windows Server 是一套服务器操作系统。本周，上述产品被披露存在远程代码执行漏洞，攻击者可利用漏洞执行任意代码。

CNVD 收录的相关漏洞包括：Microsoft Windows Remote Desktop Gateway 远程代码执行漏洞漏洞、Microsoft ASP.NET Core 远程代码执行漏洞、Microsoft Windows SMBv3 远程代码执行漏洞、Microsoft LNK 远程代码执行漏洞、Microsoft Windows Re

mote Desktop Client 远程代码执行漏洞（CNVD-2020-16712）、Microsoft Windows Graphics Device Interface 远程代码执行漏洞、Microsoft Word 远程代码执行漏洞（CNVD-2020-17174）、Microsoft Dynamics Business Central 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-2020-16110
https://www.cnvd.org.cn/flaw/show/CNVD-2020-16653
https://www.cnvd.org.cn/flaw/show/CNVD-2020-16676
https://www.cnvd.org.cn/flaw/show/CNVD-2020-16711
https://www.cnvd.org.cn/flaw/show/CNVD-2020-16712
https://www.cnvd.org.cn/flaw/show/CNVD-2020-17167
https://www.cnvd.org.cn/flaw/show/CNVD-2020-17174
https://www.cnvd.org.cn/flaw/show/CNVD-2020-17180

2、Cisco 产品安全漏洞

Cisco Integrated Management Controller（IMC）是一套用于对 UCS（统一计算系统）进行管理的软件。Cisco WebEx Network Recording Player 是用于回放在在线会议参加者的计算机上记录的 WebEx 会议记录的应用程序。Cisco Webex Player 是 Cisco 的用于播放视频会议记录的播放器。Cisco Nexus 9000 Series Fabric Switches 是一款 9000 系列光纤交换机。Cisco Smart Software Manager On-Prem 是一款用于 Cisco 产品许可证管理的组件。Cisco IOS XR Software 是美国思科（Cisco）公司的 IOS 软件系列（包括 IOS T、IOS S 和 IOS XR）中的一套完全模块化、分布式的网络操作系统。Cisco Firepower Threat Defense（FTD）是一套提供下一代防火墙服务的统一软件。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞提升权限，执行任意代码或造成拒绝服务等。

CNVD 收录的相关漏洞包括：Cisco Integrated Management Controller 权限提升漏洞、Cisco Webex Network Recording Player 和 Cisco Webex Player 缓冲区溢出漏洞（CNVD-2020-16482、CNVD-2020-16484）、Cisco Nexus 9000 Series Fabric Switches 缓冲区溢出漏洞、Cisco Smart Software Manager On-Prem 信任管理漏洞、Cisco IOS XR Software 中 Cisco Discovery 协议格式字符串漏洞、Cisco NX-OS Software 中 Cisco Discovery 协议远程代码执行漏洞、Cisco Firepower Threat Defense 访问控制错误漏洞。其中，除“Cisco Firepower Threat Defense 访问控制错误漏洞”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-2020-16474
https://www.cnvd.org.cn/flaw/show/CNVD-2020-16482
https://www.cnvd.org.cn/flaw/show/CNVD-2020-16484

https://www.cnvd.org.cn/flaw/show/CNVD-2020-16481

https://www.cnvd.org.cn/flaw/show/CNVD-2020-16485

https://www.cnvd.org.cn/flaw/show/CNVD-2020-16499

https://www.cnvd.org.cn/flaw/show/CNVD-2020-16656

https://www.cnvd.org.cn/flaw/show/CNVD-2020-16657

3、Google 产品安全漏洞

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，攻击者可利用漏洞获取敏感信息，提升权限，执行代码。

CNVD 收录的相关漏洞包括：Google Android Media Framework 代码执行漏洞（CNVD-2020-16074）、Google Android Framework 竞争条件问题漏洞、Google Android System 越界读取漏洞、Google Android System 信息泄露漏洞（CNVD-2020-17105、CNVD-2020-17107、CNVD-2020-17111、CNVD-2020-17113、CNVD-2020-17114）。其中，除“Google Android System 信息泄露漏洞（CNVD-2020-17107、CNVD-2020-17113、CNVD-2020-17114）” 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-2020-16074

https://www.cnvd.org.cn/flaw/show/CNVD-2020-17102

https://www.cnvd.org.cn/flaw/show/CNVD-2020-17105

https://www.cnvd.org.cn/flaw/show/CNVD-2020-17106

https://www.cnvd.org.cn/flaw/show/CNVD-2020-17107

https://www.cnvd.org.cn/flaw/show/CNVD-2020-17111

https://www.cnvd.org.cn/flaw/show/CNVD-2020-17113

https://www.cnvd.org.cn/flaw/show/CNVD-2020-17114

4、Qualcomm 产品安全漏洞

Qualcomm MDM9206、MDM9607、MDM9640、MDM9650、MDM9607、MSM8996AU、QCA6574AU 等都是一款中央处理器（CPU）产品。SDX24 是一款调制解调器。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受影响组件敏感信息，导致缓冲区溢出或堆溢出等。

CNVD 收录的相关漏洞包括：多款 Qualcomm 产品信息泄露漏洞（CNVD-2020-16056）、多款 Qualcomm 产品 GSNDCP Module 缓冲区溢出漏洞、多款 Qualcomm 产品 WLAN 组件缓冲区溢出漏洞、多款 Qualcomm 产品缓冲区溢出漏洞（CNVD-2020-16052、CNVD-2020-16064、CNVD-2020-16068、CNVD-2020-16070、CNVD-2020-16071）。其中，除“多款 Qualcomm 产品缓冲区溢出漏洞（CNVD-2020-16064）、多款 Qualcomm

产品 WLAN 组件缓冲区溢出漏洞”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-2020-16052
https://www.cnvd.org.cn/flaw/show/CNVD-2020-16056
https://www.cnvd.org.cn/flaw/show/CNVD-2020-16063
https://www.cnvd.org.cn/flaw/show/CNVD-2020-16064
https://www.cnvd.org.cn/flaw/show/CNVD-2020-16068
https://www.cnvd.org.cn/flaw/show/CNVD-2020-16069
https://www.cnvd.org.cn/flaw/show/CNVD-2020-16070
https://www.cnvd.org.cn/flaw/show/CNVD-2020-16071

5、BWA DiREX-Pro 远程代码执行漏洞

BWA Technology DiREX-Pro 是一款网络视频录像机。本周，BWA Technology DiREX-Pro 被披露存在远程代码执行漏洞。远程攻击者可通过向 uninstall.php3 文件发送带有 shell 元字符的‘PKG’参数利用该漏洞执行任意的操作系统命令。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-2020-17178

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-2020-16075	Zoho ManageEngine Desktop Central 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.manageengine.com/
CNVD-2020-16088	Yubico YubiKey Validation Server 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.yubico.com/support/security-advisories/ysa-2020-01/
CNVD-2020-16486	Dell EMC Isilon OneFS 访问控制错误漏洞	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.dell.com/support/security/zh-cn/details/541423/DSA-2020-039-Dell-EMC-Isilon-OneFS-Security-Update-for-a-SyncIQ-Vulnerability#resolutionsContent
CNVD-2020-16511	FasterXML Jackson jackson-databind 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://github.com/FasterXML/jackson-

			databind/commit/fc4214a883dc087070f25da738ef0d49c2f3387e
CNVD-2020-16642	Audio File Library 缓冲区溢出漏洞	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/mpruett/audiofile/commit/49103e386808042f830c18365976ad40875923ea
CNVD-2020-16718	Mozilla Firefox 进程越界写漏洞	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.mozilla.org/en-US/security/advisories/mfsa2020-05/
CNVD-2020-16838	Apache ShardingSphere 远程代码执行漏洞	高	厂商已发布相关漏洞补丁链接，请关注链接及时更新：https://github.com/apache/incubator-shardingsphere/releases
CNVD-2020-17030	eQ-3 Homematic CCU2 和 CCU3 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：http://cuxd.de/
CNVD-2020-17170	ABB eSOMS 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://new.abb.com/
CNVD-2020-17179	Froxlor 远程代码执行漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/Froxlor/Froxlor/commit/62ce21c9ec393f9962515c88f0c489ace42bf656

小结：本周，Microsoft 产品被披露存在远程代码执行漏洞，攻击者可利用漏洞执行任意代码。此外，Cisco、Google、Qualcomm 等多款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，执行任意代码，导致缓冲区溢出或堆溢出等。另外，BWA DiREX-Pro 被披露存在远程代码执行漏洞。远程攻击者可通过向 uninstall.php3 文件发送带有 shell 元字符的‘PKG’参数利用该漏洞执行任意的操作系统命令。

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、ACD Systems ACDSee Photo Studio Standard 缓冲区溢出漏洞

验证描述

ACD Systems ACDSee Photo Studio Standard 是美国 ACD Systems 公司的一套数据资产管理系统。

ACDSee Photo Studio Standard 22.1 Build 1159 版本中存在缓冲区溢出漏洞，该漏

洞源于网络系统或产品在内存上执行操作时，未正确验证数据边界，导致向关联的其他内存位置上执行了错误的读写操作，攻击者可利用该漏洞导致缓冲区溢出或堆溢出等。

验证信息

POC 链接：https://github.com/apriorit/pentesting/blob/master/bugs/acdsee_std2019/IDE_ACDStd!IEP_ShowPlugInDialog%2B0x000000000023d060.md

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2020-17037

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. 披露英特尔处理器新漏洞 Load Value Injection

研究人员披露了名叫 Load Value Injection（LVI） 的英特尔处理器新漏洞，能窃取英特尔 SGX（代表 Software Guard eXtensions）中储存的秘密信息。LVI 与 Meltdown 和 Spectre 等类似，都属于瞬态执行利用，源自于 CPU 的一项优化技术“预测执行”。

参考链接：https://www.solidot.org/story?sid=63784

2. WAGO 控制器中发现了数十个危险漏洞

思科专家发现了 WAGO 产品中的数十个漏洞，这些漏洞使控制器和人机界面（HMI）面板暴露于远程攻击之下。WAGO 是一家德国公司，专门从事电气连接和自动化解决方案。

参考链接：https://securityaffairs.co/wordpress/99430/hacking/wago-products-vulnerabilities.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