国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2020 年 04 月 20 日-2020 年 04 月 26 日　　2020 年第 17 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 533 个，其中高危漏洞 253 个、中危漏洞 217 个、低危漏洞 63 个。漏洞平均分值为 6.31。本周收录的漏洞中，涉及 0day 漏洞 297 个（占 56%），其中互联网上出现“Amovision AM-Q6320-WIFI HD Camera 远程配置泄露漏洞、Quick N Easy Web Server 拒绝服务漏洞”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 5304 个，与上周（4486 个）环比增加 18%。

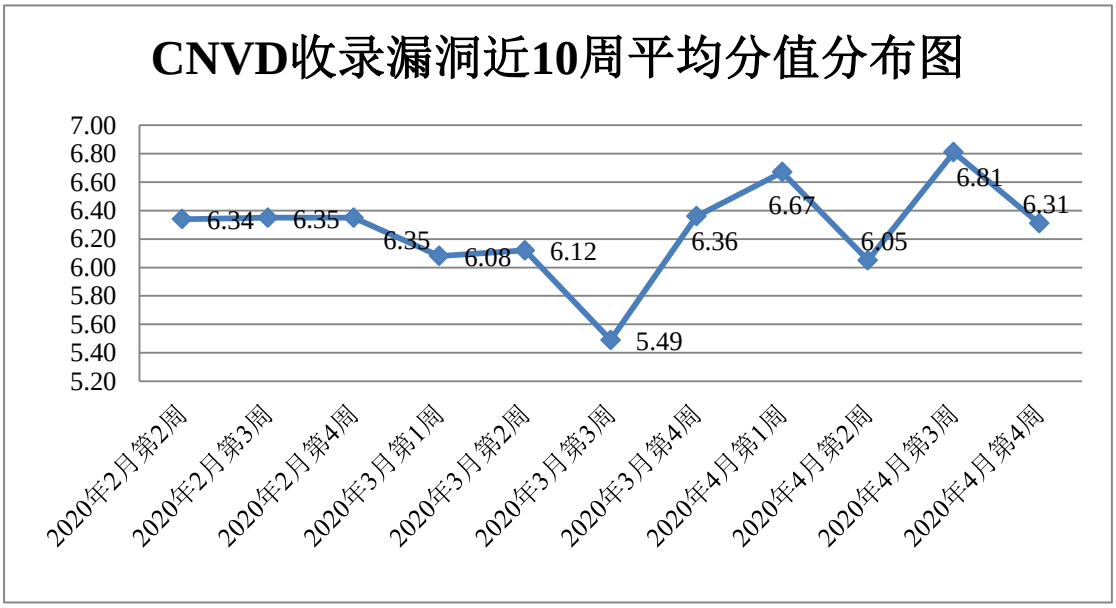

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 15 起，向基础电信企业通报漏洞事件 2 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 525 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 63 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 13 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：

荆州市华诚网络信息技术有限公司、河南跃龙门科技有限公司、上海创正信息技术有限公司、郑州维维信息技术有限公司、哈尔滨伟成科技有限公司、北京杰控科技有限公司、北京搜麦联网络科技有限公司、北京良精志诚科技有限责任公司、深圳市圆梦云科技有限公司、北京因酷时代科技有限公司、上海丹帆网络科技有限公司、欧莱雅（中国）有限公司、北京磨铁数盟信息技术有限公司、北京壹零叁玖科技发展有限公司、淄博闪灵网络科技有限公司、成都爱米秀科技有限责任公司、北京通达信科科技有限公司、深圳市科图自动化新技术应用公司、西安众邦网络科技有限公司、湖南翱云网络科技有限公司、北京英富森软件股份有限公司、江苏金智教育信息股份有限公司、湖北淘码千维信息科技有限公司、河南吉海网络科技有限公司、内蒙古浩海商贸有限公司、上海碧汉网络科技有限公司、北京逗游网络技术有限公司、武汉薄荷科技有限公司、深圳市腾讯计算机系统有限公司、上海浩方在线信息技术有限公司、厦门享游网络科技有限公司、极致网络科技有限公司、雷神（武汉）信息技术有限公司、深圳市云趣网络科技股份有限公司、南昌腾速科技有限公司、上海起凡数字技术有限公司、上海腾研信息科技有限公司、成都创想互动科技有限公司、上海起凡数字技术有限公司、上海腾研信息科技有限公司、成都创想互动科技有限公司、上海青蔓网络科技有限公司、西安德雅通科技有限公司、山西先启科技有限公司、北京世纪鼎点软件有限公司、合肥一浪网络科技有限公司、寻乌云橙信息科技有限公司、廊坊市极致网络科技有限公司、徐州海派科技有限公司、武汉号号科技有限公司、北京康邦科技有限公司、成都网旗云科信息技术有限公司、苏州恩斯特网络科技有限公司、广州盈可视电子科技有限公司、吉林省中诺科技有限公司、苏州托普斯网络科技有限公司、德国 3S 软件有限公司、上海商派网络科技有限公司、湖南潭州教育网络科技有限公司、深圳市迅雷网络技术有限公司、四川迅游网络科技股份有限公司、广州网易计算机系统有限公司、江苏友趣网络科技有限公司、上海云轴信息科技有限公司、西安佰联网络技术有限公司、海南创想未来文化传媒有限公司、中铁十四局集团房桥有限公司、全聚合网址导航、网新科技、企业第一网、施耐德（Schneider Electric）、乘风原创程序、DM 建站系统、zzz 中文网、老 y 文章管理系统、狂雨小说 cms、WMCMS 团队、Waychar、Xnview、YCCMS、SeaCMS、SemCms、ZhiCms、KKCMS、HisiPHP 和 Heybbs。

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、恒安嘉新(北京)科技股份公司、哈尔滨安天科技集团股份有限公司、华为技术有限公司、北京启明星辰信息安全技术有限公司等单位报送公开收集的漏洞数量较多。北京华云安信息技术有限公司、北京铭图天成信息技术有限公司、山东新潮信息技术有限公司、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、上海观安信息技术股份有限公司、成都链安科技有限公司、长春嘉诚信息技术股份有限公司、河南灵创电子科技有限公司、国瑞数码零点实验室、广州安亿信软件科技有限公司、山东云天安全技术有限公司、深圳市魔方安全科技有限公司、河南信安世纪科技有限公司、四川月安客信息技术有限公司、西安秦易信息技术有限公司、博智安全科技股份有限公司、北京丁牛科技有限公司、鼎信信息科技有限责任公司、南方电网数字电网研究院有限公司、北京机沃科技有限公司、北京智游网安科技有限公司、北京浩瀚深度信息技术股份有限公司、北京墨云科技有限公司、成都安美勤信息技术股份有限公司及其他个人白帽子向 CNVD 提交了 5304 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 4013 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）	2197	2197
上海交大	960	960
奇安信网神（补天平台）	856	856
北京天融信网络安全技术有限公司	520	6
恒安嘉新(北京)科技股份公司	423	0
哈尔滨安天科技集团股份有限公司	316	0
华为技术有限公司	145	0
北京启明星辰信息安全技术有限公司	133	20
新华三技术有限公司	93	0
北京神州绿盟科技有限公司	89	21
中新网络信息安全股份有限公司	57	57
深信服科技股份有限公司	54	0

西安四叶草信息技术有限公司	23	23
杭州安恒信息技术股份有限公司	20	20
北京奇虎科技有限公司	16	0
中国电信集团系统集成有限责任公司	14	14
北京安信天行科技有限公司	10	10
北京知道创宇信息技术股份有限公司	3	0
北京华云安信息技术有限公司	111	111
北京铭图天成信息技术有限公司	96	96
山东新潮信息技术有限公司	87	87
远江盛邦（北京）网络安全科技股份有限公司	77	77
南京众智维信息科技有限公司	63	63
上海观安信息技术股份有限公司	51	51
成都链安科技有限公司	37	37
杭州迪普科技股份有限公司	35	0
长春嘉诚信息技术股份有限公司	33	33
河南灵创电子科技有限公司	32	32
国瑞数码零点实验室	17	17
广州安亿信软件科技有限公司	5	5
山东云天安全技术有限公司	4	4
深圳市魔方安全科技有限公司	4	4
河南信安世纪科技有限公司	3	3
四川月安客信息技术有限公司	3	3

西安秦易信息技术有限公司	3	3
博智安全科技股份有限公司	2	2
北京丁牛科技有限公司	2	2
鼎信信息科技有限责任公司	2	2
南方电网数字电网研究院有限公司	2	2
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
北京浩瀚深度信息技术股份有限公司	1	1
北京墨云科技有限公司	1	1
成都安美勤信息技术股份有限公司	1	1
CNCERT 青海分中心	4	4
CNCERT 海南分中心	1	1
CNCERT 吉林分中心	1	1
个人	475	475
报送总计	7084	5304

本周漏洞按类型和厂商统计

本周，CNVD 收录了 533 个漏洞。应用程序 211 个，WEB 应用 210 个，网络设备（交换机、路由器等网络端设备）39 个，操作系统 19 个，安全产品 16 个，数据库 26 个，智能设备（物联网终端设备）漏洞 10 个，区块链 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	211
WEB 应用	210
网络设备（交换机、路由器等网络端设备）	39
操作系统	19
安全产品	16

数据库	26
智能设备（物联网终端设备）漏洞	10
区块链	2

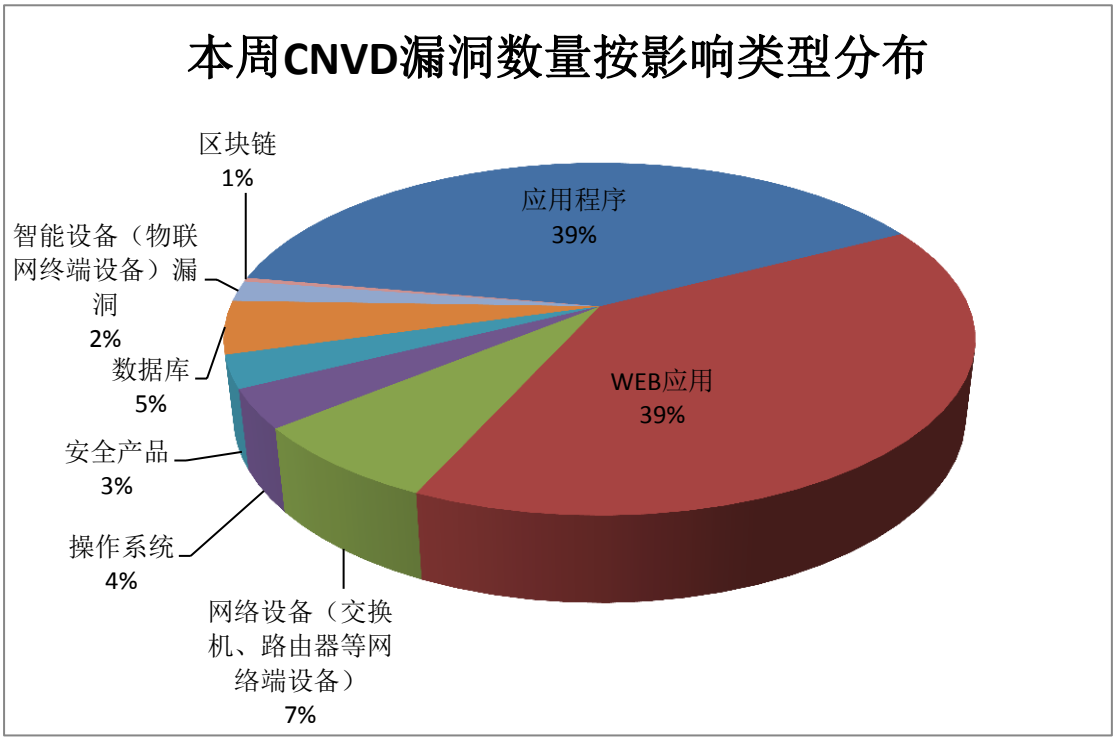

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Oracle、Microsoft、Foxit 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	60	11%
2	Microsoft	28	5%
3	Foxit	25	5%
4	NETGEAR	22	4%
5	湖北淘码千维信息科技有限公司	12	2%
6	Mcafee	11	2%
7	Google	11	2%
8	Industrial Light and Magic	8	2%
9	SAP	8	2%
10	其他	348	65%

本周行业漏洞收录情况

本周，CNVD 收录了 60 个电信行业漏洞，22 个移动互联网行业漏洞，13 个工控行业漏洞（如下图所示）。其中，“NETGEAR MR1100 输入验证错误漏洞、Oracle MySQL Server 拒绝服务漏洞（CNVD-2020-23465）、TP-Link Archer A7 AC1750 授权问题漏洞（CNVD-2020-24409）、Google Android System 越界写入漏洞（CNVD-2020-24776）、ABB System 800xA Base 授权问题漏洞”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/

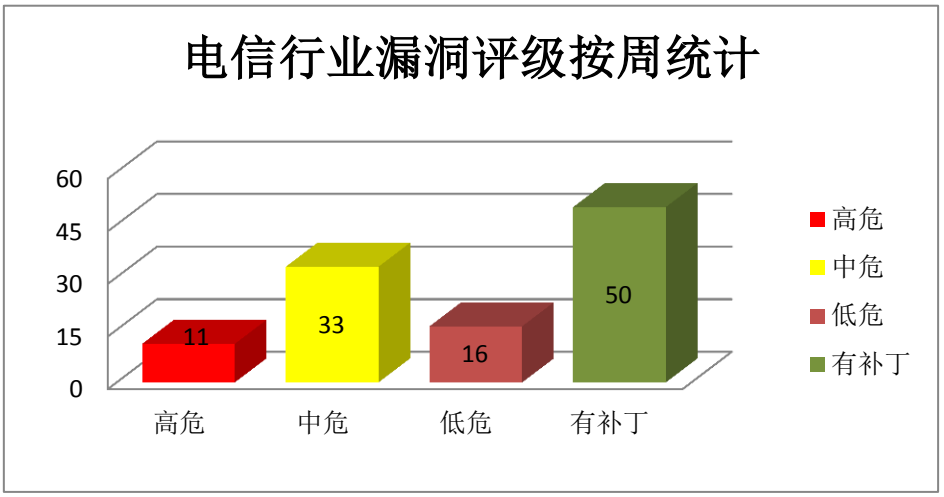

图 3 电信行业漏洞统计

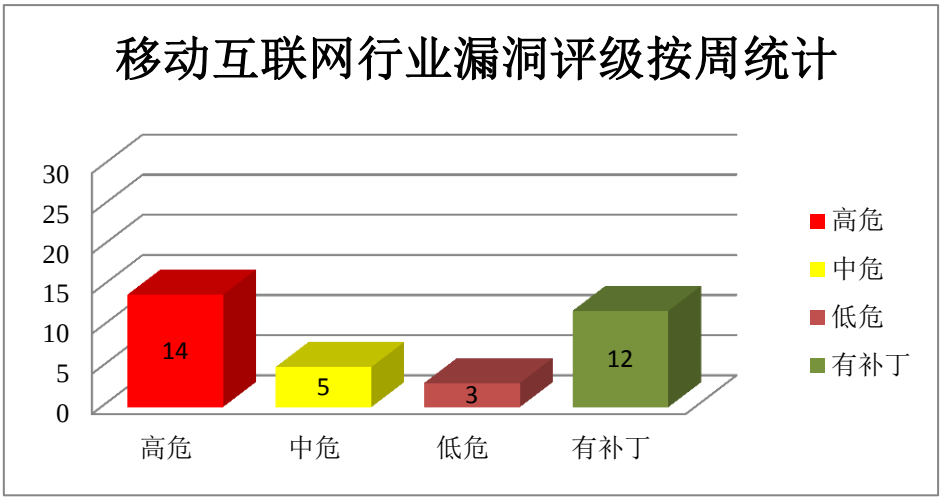

图 4 移动互联网行业漏洞统计

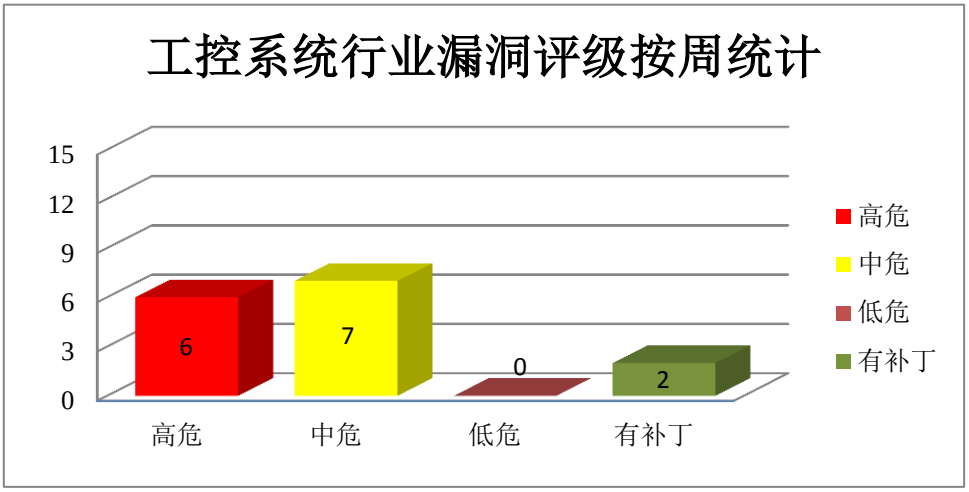

图 5 工控系统行业漏洞统计

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、Oracle 产品安全漏洞

Oracle MySQL 是一套开源的关系数据库管理系统。Oracle Retail Applications 是一套零售应用商店解决方案。Oracle E-Business Suite（电子商务套件）是一套全面集成式的全球业务管理软件。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞影响数据的可用性、保密性和完整性。

CNVD 收录的相关漏洞包括：Oracle MySQL Server 拒绝服务漏洞（CNVD-2020-23461、CNVD-2020-23460、CNVD-2020-23465）、Oracle 访问控制错误漏洞、Oracle E-Business Suite Email Center 未授权操作漏洞（CNVD-2020-23751）、Oracle E-Business Suite Marketing Encyclopedia System 未授权操作漏洞、Oracle E-Business Suite General Ledger 未授权访问漏洞、Oracle E-Business Suite Email Center 未授权操作漏洞。除“Oracle MySQL Server 拒绝服务漏洞（CNVD-2020-23461、CNVD-2020-23460）”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-2020-23461

https://www.cnvd.org.cn/flaw/show/CNVD-2020-23460

https://www.cnvd.org.cn/flaw/show/CNVD-2020-23465

https://www.cnvd.org.cn/flaw/show/CNVD-2020-23744

https://www.cnvd.org.cn/flaw/show/CNVD-2020-23751

https://www.cnvd.org.cn/flaw/show/CNVD-2020-23750

https://www.cnvd.org.cn/flaw/show/CNVD-2020-23753

https://www.cnvd.org.cn/flaw/show/CNVD-2020-23752

2、Microsoft 产品安全漏洞

Microsoft SharePoint 是一套企业业务协作平台。Microsoft Office 是的一款办公软件套件产品。Microsoft Word 是一套 Office 套件中的文字处理软件。Microsoft AutoUpdate for Mac 是一款适用于 Mac 的自动升级组件。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。Windows Update Client 是其中的一个 Windows 系统更新客户端。Microsoft Excel 是一款 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，攻击者可利用漏洞提升权限，执行任意代码。

CNVD 收录的相关漏洞包括：icrosoft SharePoint 远程代码执行漏洞（CNVD-2020-24060、CNVD-2020-24062）、Microsoft Office Access Connectivity Engine 远程代码执行漏洞（CNVD-2020-24065）、Microsoft Word 远程代码执行漏洞（CNVD-2020-24069）、Microsoft AutoUpdate for Mac 提权漏洞、Microsoft Windows Update Client 提权漏洞、Microsoft Windows Graphics Components 远程代码执行漏洞、Microsoft Excel 远程代码执行漏洞（CNVD-2020-24131）。其中，除“Microsoft SharePoint 远程代码执行漏洞（CNVD-2020-24060、CNVD-2020-24062）”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-2020-24060
https://www.cnvd.org.cn/flaw/show/CNVD-2020-24062
https://www.cnvd.org.cn/flaw/show/CNVD-2020-24065
https://www.cnvd.org.cn/flaw/show/CNVD-2020-24069
https://www.cnvd.org.cn/flaw/show/CNVD-2020-24071
https://www.cnvd.org.cn/flaw/show/CNVD-2020-24073
https://www.cnvd.org.cn/flaw/show/CNVD-2020-24132
https://www.cnvd.org.cn/flaw/show/CNVD-2020-24131

3、Foxit 产品安全漏洞

Foxit Reader 和 Foxit PhantomPDF 都是中国福昕（Foxit）公司的一款 PDF 文档阅读器。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞在当前进程的上下文中执行任意代码。

CNVD 收录的相关漏洞包括：Foxit Reader 和 PhantomPDF 类型混淆远程代码执行漏洞（CNVD-2020-24443、CNVD-2020-24446、CNVD-2020-24445、CNVD-2020-24444）、Foxit Reader 和 PhantomPDF 任意文件写入漏洞、Foxit Reader 和 PhantomPDF communication API 任意文件写入漏洞、Foxit Reader 和 PhantomPDF 资源管理错误漏洞（CNVD-2020-24461、CNVD-2020-24465）。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-2020-24443

https://www.cnvd.org.cn/flaw/show/CNVD-2020-24446

https://www.cnvd.org.cn/flaw/show/CNVD-2020-24445

https://www.cnvd.org.cn/flaw/show/CNVD-2020-24444

https://www.cnvd.org.cn/flaw/show/CNVD-2020-24454

https://www.cnvd.org.cn/flaw/show/CNVD-2020-24453

https://www.cnvd.org.cn/flaw/show/CNVD-2020-24461

https://www.cnvd.org.cn/flaw/show/CNVD-2020-24465

4、Google 产品安全漏洞

Google Closure Library 是一款跨浏览器的、模块化的 JavaScript 库。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，攻击者可利用漏洞提升权限，获取非法授权，执行代码。

CNVD 收录的相关漏洞包括：Google Closure Library 输入验证错误漏洞、Google Android System 越界写入漏洞（CNVD-2020-24773、CNVD-2020-24776、CNVD-2020-24775、CNVD-2020-24774）、Google Android FPC Iris TZ App 越界写入漏洞、Google Android FPC Iris TZ App 越界读取漏洞、Google Android Media framework 越界写入漏洞。其中，除“Google Android FPC Iris TZ App 越界写入漏洞、Google Android FPC Iris TZ App 越界读取漏洞、Google Android Media framework 越界写入漏洞”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-2020-24030

https://www.cnvd.org.cn/flaw/show/CNVD-2020-24773

https://www.cnvd.org.cn/flaw/show/CNVD-2020-24772

https://www.cnvd.org.cn/flaw/show/CNVD-2020-24770

https://www.cnvd.org.cn/flaw/show/CNVD-2020-24776

https://www.cnvd.org.cn/flaw/show/CNVD-2020-24775

https://www.cnvd.org.cn/flaw/show/CNVD-2020-24774

https://www.cnvd.org.cn/flaw/show/CNVD-2020-24778

5、ABB Telephone Gateway TG/S 和 Busch-Jaeger Telefon-Gateway 权限许可和访问控制问题漏洞

ABB Telephone Gateway TG/S 和 Busch-Jaeger 6186/11 Telefon-Gateway 都是瑞士 ABB 公司的一款电话网关产品。本周，ABB Telephone Gateway TG/S 3.2 版本和 Busch-Jaeger 6186/11 Telefon-Gateway 被披露存在权限许可证和访问控制漏洞。该漏洞源于

访问控制不当。攻击者可利用该漏洞访问受限数据。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-2020-25010

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-2020-23481	Trend Micro Security 代码执行漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://esupport.trendmicro.com/en-us/home/pages/technical-support/1124031.aspx
CNVD-2020-24011	Draytek VigorAP910C 信息泄露漏洞	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.draytek.com/
CNVD-2020-24015	IBM InfoSphere Information Server 权限提升漏洞（CNVD-2020-24015）	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.ibm.com/support/pages/node/6191679
CNVD-2020-24029	OTRS 信息泄露漏洞（CNVD-2020-24029）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://otrs.com/release-notes/otrs-security-advisory-2020-09/
CNVD-2020-24027	F5 BIG-IP 输入验证错误漏洞（CNVD-2020-24027）	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.f5.com/csp/article/K01054113
CNVD-2020-24033	FasterXML jackson-databind 代码问题漏洞（CNVD-2020-24033）	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/issues/2662
CNVD-2020-24030	Google Closure Library 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://github.com/google/closure-library/releases/tag/v20200315
CNVD-2020-24421	NETGEAR MR1100 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：https://kb.netgear.com/000061460/Security-Advisory-for-Missing-Function-Level-Access-Control-on-MR1100-PSV-2018-0537

CNVD-2020-23480	Trend Micro Security 2019 (Consumer)任意代码执行漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://esupport.trendmicro.com/en-us/home/pages/technical-support/1124090.aspx
CNVD-2020-24026	F5 BIG-IP 缓冲区错误漏洞	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.f5.com/csp/article/K22113131

小结：本周，Oracle 产品被披露存在多个漏洞，攻击者可利用漏洞影响数据的可用性、保密性和完整性。此外 Microsoft、Foxit、Google 等多款产品被披露存在多个漏洞，攻击者可利用漏洞提升权限，获取非法授权，执行代码。另外，ABB Telephone Gateway TG/S 和 Busch-Jaeger Telefon-Gateway 被披露存在权限许可和访问控制问题漏洞。攻击者可利用该漏洞访问受限数据。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、Amovision AM-Q6320-WIFI HD Camera 远程配置泄露漏洞

验证描述

Amovision AM-Q6320-WIFI HD Camera 是一款高清摄像头。

Amovision AM-Q6320-WIFI HD Camera 存在远程配置泄露漏洞。攻击者可利用漏洞泄露敏感信息。

验证信息

POC 链接：https://www.exploitalert.com/view-details.html?id=34994

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2020-24044

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. FPGA 芯片被曝严重的 Starbleed 漏洞，影响数据中心 IoT 工业设备等

学术研究团队表示，他们在世界行业巨头 Xilinx 生产的 FPGA (Field Programma

ble Gate Arrays) 芯片集中发现了一个新型安全漏洞 “Starbleed”，可导致具有物理或远程访问权限的攻击者提取并篡改 FGPA 比特流（配置文件）以恶意代码重新编写芯片。

参考链接：https://mp.weixin.qq.com/s/PE-c6VkuOC-8K3RTmCEMFA

2. 新款 iPhone SE 开售前夕，iOS 被曝存在八年的 0day 漏洞

近日，安全研究人员发现 iPhone 和 iPad 自带的默认邮件应用程序 MobileMail 和 Maild 存在两个正在被利用的严重漏洞，而且至少在两年前就已经开始监视用户了。

参考链接：https://www.freebuf.com/news/234727.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