国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2020 年 06 月 01 日-2020 年 06 月 07 日　　2020 年第 23 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 465 个，其中高危漏洞 150 个、中危漏洞 255 个、低危漏洞 60 个。漏洞平均分值为 5.72。本周收录的漏洞中，涉及 0day 漏洞 190 个（占 41%），其中互联网上出现“SolarWinds Orion Platform 信息泄露漏洞、Zoom Call Recording 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 3065 个，与上周（3956 个）环比减少 23%。

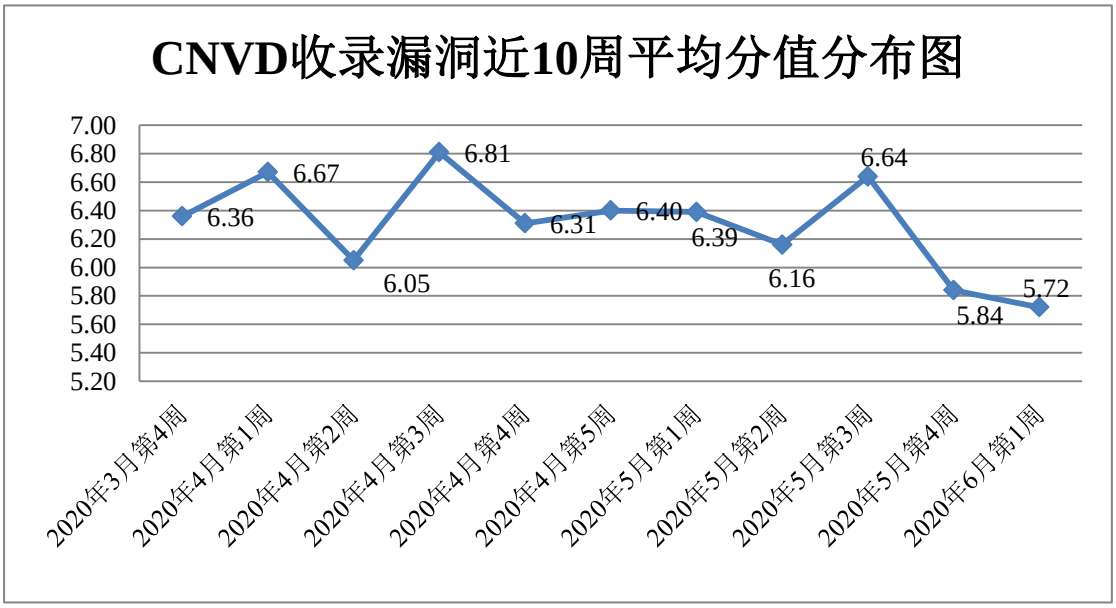

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 11 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 197 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 29 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 20 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：

铭飞科技有限公司、成都维熵科技有限责任公司、西安三才科技实业有限公司、安科瑞电气股份有限公司、云康健康产业投资股份有限公司、北京良精志诚科技有限责任公司、深圳锟铻科技有限公司、朋友圈网络科技有限公司、海南赞赞网络科技有限公司、廊坊市极致网络科技有限公司、深圳市富士智能系统有限公司、苏州聚尚网络科技有限公司、湖南翱云网络科技有限公司、深圳市锟铻科技有限公司、石家庄市征红网络科技有限公司、重庆逐越光电科技有限公司、青岛自动化仪表有限公司、浙江慕枫网站科技有限公司、长沙米拓信息技术有限公司、镇江市云优网络科技有限公司、苏州托普斯网络科技有限公司、用友网络科技股份有限公司、中山市中贸网络信息有限公司、锐捷网络股份有限公司、青岛易企天创管理咨询有限公司、上海博达数据通信有限公司、广联达科技股份有限公司、广州市互诺计算机科技有限公司、深圳市圆梦云科技有限公司、四平市九州易通科技有限公司、上海泛微网络科技股份有限公司、广州市保伦电子有限公司、上海覆盆子信息科技有限公司、开平市联科网络科技有限公司、茉柏枘（上海）软件科技有限公司、河南跃龙门科技有限公司、苏州乐艺网络科技有限公司、南京润洽网络科技有限公司、淄博闪灵网络科技有限公司、苏州乐艺网络科技有限公司、南京润洽网络科技有限公司、三一网络技术有限公司、苏州天啸网络科技有限公司、南京遂腾网络科技有限公司、北京菲斯特诺科技有限公司、成都任我行软件股份有限公司、首岳資訊網路股份有限公司、珠海金山办公软件有限公司、北京二六三企业通信有限公司、深圳银澎云计算有限公司、全时云商务服务股份有限公司、北京小鱼易连科技有限公司、中粮集团有限公司、北京中铁十八局集团有限公司、精灵在线网络技术(北京)有限公司、济南亘安信息技术有限公司、深圳市硕赢互动信息技术有限公司、中金金融认证中心有限公司、南京旭步网络科技有限公司、芜湖易讯信息技术有限公司、浙江浙大中控信息技术有限公司、沧州市凡诺广告传媒有限公司、南昌正能信息技术有限公司、福州凌夕网络科技有限公司、济南宇霞信息技术有限公司、研华科技（中国）有限公司、合肥奇乐网络科技有限公司、长沙德尚网络科技有限公司、深圳市国人在线信息技术有限公司、深圳市吉祥腾达科技有限公司、江下信息科技（惠州）有限公司、Emerson 公司、新秀科技、网展科技、校无忧科技、Lerx 网络科技、北京市大兴区科学技术协会、中国医药保健品进出口商会、上海荃路软件开发工作室、飞飞影视导航系统、ZrLog 博客、HadSky、YCCMS、ImageMagick Studio LLC、Monstra、Emlog、Emerson、Jfinal cms、ZZCMS、BEESCMS、Uublog、Freecms、The Apache Software Foundation 和 Phpcms。

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，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、新华三技术有限公司、华为技术有限公司、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。国瑞数码零点实验室、远江盛邦（北京）网络安全科技股份有限公司、山东新潮信息技术有限公司、河南灵创电子科技有限公司、杭州迪普科技股份有限公司、山东云天安全技术有限公司、河南信安世纪科技有限公司、成都安美勤信息技术股份有限公司、上海观安信息技术股份有限公司、京东云安全、北京禹宏信安科技有限公司、河北华测信息技术有限公司、北京长亭科技有限公司、上海纽盾科技股份有限公司、北京顶象技术有限公司、北京浩瀚深度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、山东道普测评技术有限公司、上海上讯信息技术股份有限公司、江苏省信息安全测评中心、国家互联网应急中心、北京智游网安科技有限公司、吉林谛听信息技术有限公司及其他个人白帽子向 CNVD 提交了 3065 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 2394 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）	1140	1140
奇安信网神（补天平台）	898	898
恒安嘉新(北京)科技股份公司	438	0
上海交大	356	356
哈尔滨安天科技集团股份有限公司	268	0
新华三技术有限公司	207	0
华为技术有限公司	176	0
北京天融信网络安全技术有限公司	128	9
深信服科技股份有限公司	92	1
北京奇虎科技有限公司	81	72
北京神州绿盟科技有限公司	66	0
北京启明星辰信息安全技术有限公司	57	1

国瑞数码零点实验室	51	51
远江盛邦（北京）网络安全科技股份有限公司	30	30
山东新潮信息技术有限公司	26	26
河南灵创电子科技有限公司	23	23
杭州迪普科技股份有限公司	15	15
山东云天安全技术有限公司	10	10
河南信安世纪科技有限公司	10	10
成都安美勤信息技术股份有限公司	5	5
上海观安信息技术股份有限公司	4	4
京东云安全	4	4
北京禹宏信安科技有限公司	4	4
河北华测信息技术有限公司	4	4
北京长亭科技有限公司	3	3
上海纽盾科技股份有限公司	2	2
北京顶象技术有限公司	2	2
北京浩瀚深度信息技术股份有限公司	2	2
北京圣博润高新技术股份有限公司	2	2
山东道普测评技术有限公司	2	2
上海上讯信息技术股份有限公司	1	1
江苏省信息安全测评中心	1	1
国家互联网应急中心	1	1
北京智游网安科技有限公司	1	1

吉林谛听信息技术有限公司	1	1
CNCERT 天津分中心	23	23
CNCERT 青海分中心	6	6
CNCERT 西藏分中心	3	3
CNCERT 宁夏分中心	1	1
CNCERT 河北分中心	1	1
个人	350	350
报送总计	4495	3065

本周漏洞按类型和厂商统计

本周，CNVD 收录了 465 个漏洞。应用程序 180 个，WEB 应用 126 个，操作系统 97 个，网络设备（交换机、路由器等网络端设备）40 个，安全产品 15 个，智能设备（物联网终端设备）5 个，数据库 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	180
WEB 应用	126
操作系统	97
网络设备（交换机、路由器等网络端设备）	40
安全产品	15
智能设备（物联网终端设备）	5
数据库	2

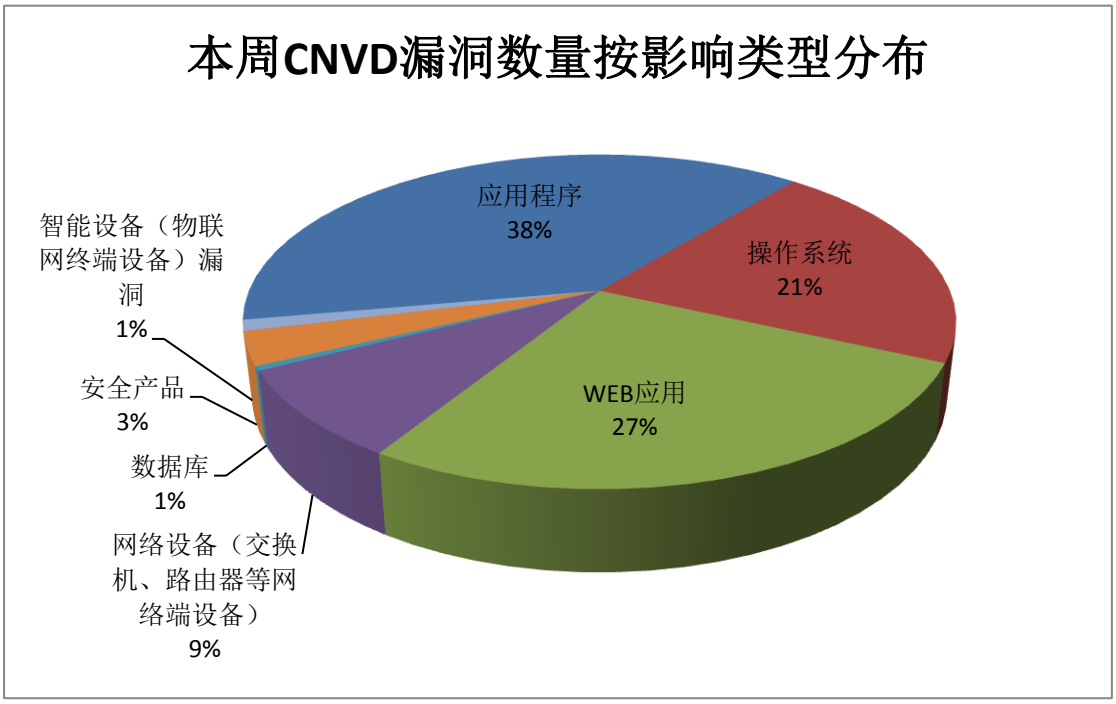

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Google、NETGEAR、IBM 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	Google	69	15%
2	NETGEAR	27	6%
3	IBM	24	5%
4	Xnview	19	4%
5	Microsoft	19	4%
6	FreeRDP	16	3%
7	Cisco	12	3%
8	Dell	11	2%
9	Palo Alto Networks	10	2%
10	其他	258	56%

本周行业漏洞收录情况

本周，CNVD 收录了 40 个电信行业漏洞，76 个移动互联网行业漏洞，12 个工控行业漏洞（如下图所示）。其中，“Google Android Framework 权限提升漏洞（CNVD-2020-31529）、Samsung 移动设备加密问题漏洞”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/

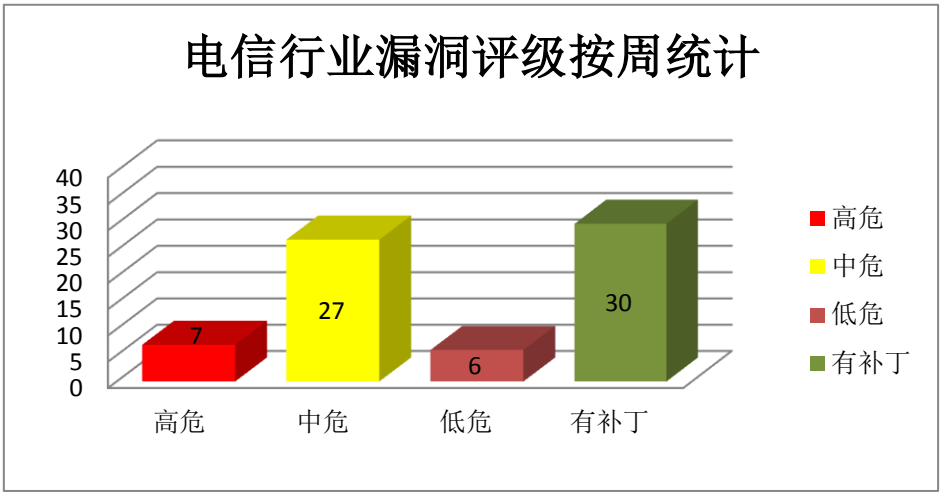

图 3 电信行业漏洞统计

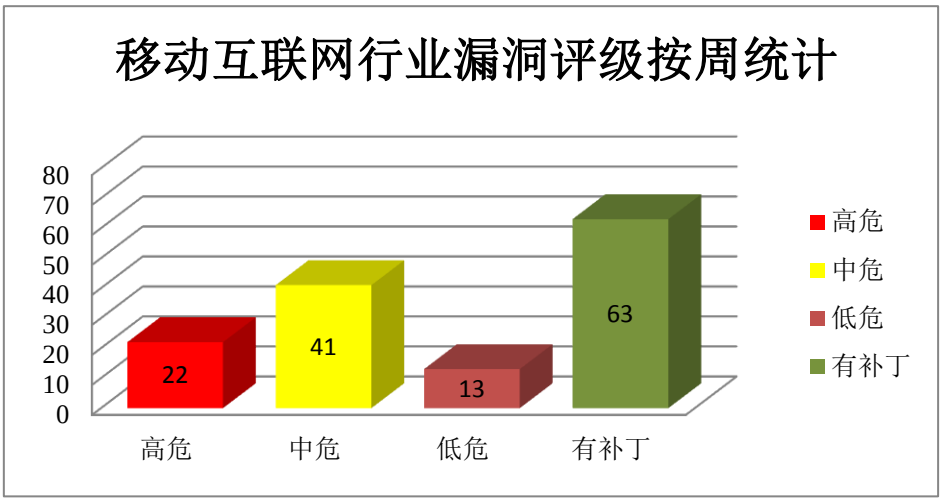

图 4 移动互联网行业漏洞统计

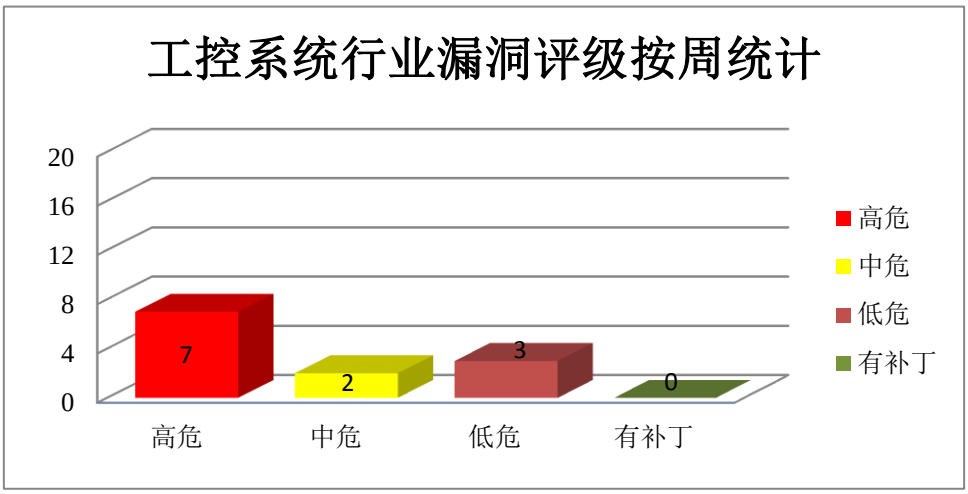

图 5 工控系统行业漏洞统计

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 Window 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。Microsoft Internet Explorer（IE）是一款 Windows 操作系统附带的 Web 浏览器。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，损坏内存。

CNVD 收录的相关漏洞包括：Microsoft VBScript 引擎远程命令执行漏洞、Microsoft Windows 远程命令执行漏洞、Microsoft Windows Jet Database Engine 缓冲区溢出漏洞、Microsoft Windows DirectX 权限提升漏洞（CNVD-2020-31542）、Microsoft Windows Hyper-V 权限提升漏洞（CNVD-2020-31546）、Microsoft Windows Kernel 权限提升漏洞（CNVD-2020-31545）、Microsoft Windows User-Mode Power Service 权限提升漏洞、Microsoft Internet Explorer VBScript Engine 缓冲区溢出漏洞。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-2020-31122
https://www.cnvd.org.cn/flaw/show/CNVD-2020-31126
https://www.cnvd.org.cn/flaw/show/CNVD-2020-31127
https://www.cnvd.org.cn/flaw/show/CNVD-2020-31542
https://www.cnvd.org.cn/flaw/show/CNVD-2020-31546
https://www.cnvd.org.cn/flaw/show/CNVD-2020-31545
https://www.cnvd.org.cn/flaw/show/CNVD-2020-31549
https://www.cnvd.org.cn/flaw/show/CNVD-2020-31548

2、Dell 产品安全漏洞

Dell EMC Isilon OneFS 是一套适用于非结构化数据的横向扩展存储系统。Dell EMC RSA Archer 是一款企业 IT 治理和合规治理产品。Dell OS recovery 是一款系统恢复软件。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞获取受影响组件敏感信息，执行任意命令等。

CNVD 收录的相关漏洞包括：Dell EMC Isilon OneFS 安全特征问题漏洞（CNVD-2020-31248、CNVD-2020-31249）、Dell EMC RSA Archer 信息泄露漏洞（CNVD-2020-31252）、Dell EMC RSA Archer 操作系统命令注入漏洞、Dell EMC RSA Archer 跨站请求伪造漏洞、Dell EMC RSA Archer 跨站脚本漏洞、Dell EMC RSA Archer 输入验

证错误漏洞、Dell OS recovery 未授权访问漏洞。其中，“Dell EMC RSA Archer 操作系统命令注入漏洞、Dell OS recovery 未授权访问漏洞”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-2020-31248
https://www.cnvd.org.cn/flaw/show/CNVD-2020-31249
https://www.cnvd.org.cn/flaw/show/CNVD-2020-31252
https://www.cnvd.org.cn/flaw/show/CNVD-2020-31251
https://www.cnvd.org.cn/flaw/show/CNVD-2020-31254
https://www.cnvd.org.cn/flaw/show/CNVD-2020-31253
https://www.cnvd.org.cn/flaw/show/CNVD-2020-31256
https://www.cnvd.org.cn/flaw/show/CNVD-2020-31257

3、Cisco 产品安全漏洞

Cisco Firepower Threat Defense 是一套提供下一代防火墙服务的统一软件。Cisco Adaptive Security Appliances Software 是一套防火墙和网络安全平台。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，造成拒绝服务。

CNVD 收录的相关漏洞包括：Cisco Firepower Threat Defense 和 Adaptive Security Appliances Software 拒绝服务漏洞（CNVD-2020-31105、CNVD-2020-31104、CNVD-2020-31111、CNVD-2020-31110、CNVD-2020-31114）、Cisco Firepower Threat Defense 和 Adaptive Security Appliances Software 内存泄漏漏洞、Cisco Firepower Threat Defense 拒绝服务漏洞、Cisco Firepower Threat Defense 和 Adaptive Security Appliances Software 信息泄露漏洞。其中，“Cisco Firepower Threat Defense 和 Adaptive Security Appliances Software 拒绝服务漏洞（CNVD-2020-31105、CNVD-2020-31111、CNVD-2020-31110）”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-2020-31105
https://www.cnvd.org.cn/flaw/show/CNVD-2020-31104
https://www.cnvd.org.cn/flaw/show/CNVD-2020-31103
https://www.cnvd.org.cn/flaw/show/CNVD-2020-31107
https://www.cnvd.org.cn/flaw/show/CNVD-2020-31106
https://www.cnvd.org.cn/flaw/show/CNVD-2020-31111
https://www.cnvd.org.cn/flaw/show/CNVD-2020-31110
https://www.cnvd.org.cn/flaw/show/CNVD-2020-31114

4、IBM 产品安全漏洞

IBM Security Identity Governance and Intelligence（IGI）是一套身份治理解决方案。

IBM Spectrum Scale 是一套基于 IBM GPFS（专为 PB 级存储管理而优化的企业文件管理系统）的可扩展的数据及文件管理解决方案。IBM MobileFirst Platform Foundation 是一套移动应用程序管理解决方案。IBM Sterling B2B Integrator 是一套集成了重要的 B2B 流程、交易和关系的软件。IBM Security Identity Governance and Intelligence（IGI）是一套身份治理解决方案。本周，上述产品被披露存在信息泄露漏洞，攻击者可利用漏洞获取敏感信息。

CNVD 收录的相关漏洞包括：IBM Security Identity Governance and Intelligence 信息泄露漏洞（CNVD-2020-30830、CNVD-2020-30831、CNVD-2020-31092、CNVD-2020-31574）、IBM Spectrum Scale 信息泄露漏洞（CNVD-2020-30834）、IBM MobileFirst Platform Foundation 信息泄露漏洞、IBM Sterling B2B Integrator 信息泄露漏洞（CNVD-2020-30842、CNVD-2020-31094）。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-2020-30830

https://www.cnvd.org.cn/flaw/show/CNVD-2020-30831

https://www.cnvd.org.cn/flaw/show/CNVD-2020-30834

https://www.cnvd.org.cn/flaw/show/CNVD-2020-30837

https://www.cnvd.org.cn/flaw/show/CNVD-2020-30842

https://www.cnvd.org.cn/flaw/show/CNVD-2020-31092

https://www.cnvd.org.cn/flaw/show/CNVD-2020-31094

https://www.cnvd.org.cn/flaw/show/CNVD-2020-31574

5、多款 Tenda 产品缓冲区溢出漏洞（CNVD-2020-31409）

Tenda AC9 等都是中国腾达（Tenda）公司的一款无线路由器。本周，多款 Tenda 产品被披露存在缓冲区溢出漏洞。攻击者可通过向/goform/SetNetControlList URL 发送‘list’参数利用该漏洞执行任意代码。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-2020-31409

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-2020-31084	Lenovo Printer LJ4010DN 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://iknow.lenovo.com.cn/detail/dc_188830.html
CNVD-2020-	SQLite 资源管理错误漏洞（C	高	目前厂商已发布升级补丁以修复漏

31117	NVD-2020-31117）		洞，补丁获取链接：https://sqlite.org/src/info/0d69f76f0865f962
CNVD-2020-31167	Sympa 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://github.com/sympa-community/sympa/releases
CNVD-2020-31284	Apple macOS Catalina Accounts 组件安全限制绕过漏洞	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/zh-cn/HT211170
CNVD-2020-31526	Google Android Media framework 权限提升漏洞（CNVD-2020-31526）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://source.android.com/security/bulletin/2020-06-01
CNVD-2020-31589	Palo Alto Networks PAN-OS SD WAN 组件任意代码执行漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://security.paloaltonetworks.com/CVE-2020-2009
CNVD-2020-31597	Aviatrix VPN Client 权限处理特权提升漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：https://aviatrix.com/
CNVD-2020-31602	Contiki 和 Contiki-NG 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/contiki-ng/contiki-ng/releases/tag/release%2Fv4.4
CNVD-2020-31600	F5 BIG-IQ Centralized Management 操作系统命令注入漏洞	高	目前厂商只发布了该软件 7.x 版本的修复措施，该软件 6.x 版本的修复措施暂未发布，详情请参考链接：https://support.f5.com/csp/article/K37130415
CNVD-2020-31758	Apache Syncope 代码注入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：http://syncope.apache.org/security

小结：本周，Microsoft 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，损坏内存。此外 Dell、Cisco、IBM 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，执行任意命令，造成拒绝服务等。另外，多款 Tenda 产品被披露存在缓冲区溢出漏洞。攻击者可通过向/goform/SetNetControlList URL 发送‘list’参数利用该漏洞执行任意代码。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、Zoom Call Recording 跨站脚本漏洞

验证描述

Zoom Call Recording 是美国 Zoom 公司的一套可扩展的会话记录管理解决方案。该产品支持记录、管理和查找会话记录等功能。

Zoom Call Recording 6.3.1 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://github.com/DrunkenShells/Disclosures/tree/master/CVE-2019-18223-XSS-ZoomCallRecording

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2020-31541

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. SAP ASE 漏洞可能使攻击者入侵数据库服务器

网络安全公司 Trustwave 披露了六个漏洞，它们存在于 Sybase Adaptive Server Enterprise（ASE）中，后者是一种面向基于事务的应用程序的关系数据库管理软件，可以使无特权的攻击者在某些情况下完全控制目标数据库，甚至是底层操作系统。

参考链接：https://thehackernews.com/2020/06/newly-patched-sap-ase-flaws-could-let.html

2. 研究人员披露苹果登录系统的一个严重漏洞

安全研究员 Bhavuk Jainb 曝出了苹果登录系统的一个严重漏洞，该漏洞可被用来访问从 Dropbox，Spotify 到 Airbnb 站点上的帐户。

参考链接：https://www.theregister.com/2020/06/01/flaw_apple_sso/

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