国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2020 年 08 月 24 日-2020 年 08 月 30 日　　2020 年第 35 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 673 个，其中高危漏洞 289 个、中危漏洞 329 个、低危漏洞 55 个。漏洞平均分值为 6.14。本周收录的漏洞中，涉及 0day 漏洞 480 个（占 71%），其中互联网上出现“LimeSurvey 'Survey Menu'存储型跨站脚本漏洞、ZKTeco FaceDepot 和 ZKBiosecurity Server 令牌重用漏洞”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 4604 个，与上周（3061 个）环比增加 50%。

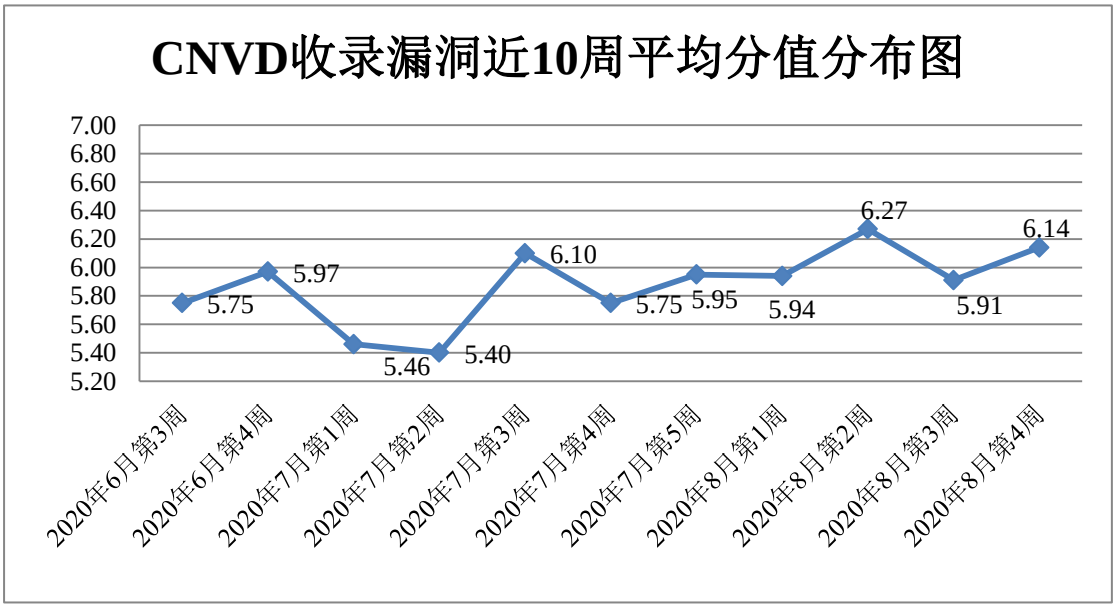

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 514 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 28 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：

广东快乐种子科技有限公司、普联技术有限公司、深圳市睿视科技有限公司、昆明云涛科技有限公司、珠海金山办公软件有限公司、研华科技（中国）有限公司、锐捷网络股份有限公司、济南卓源软件有限公司、深圳市中联创新自控系统有限公司、海南易而优科技有限公司、北京通达志成科技有限公司、福建福昕软件开发股份有限公司、杭州迪普科技股份有限公司、石家庄捷搜网络科技有限公司、宜兴易发网络服务有限公司、上海纵之格科技有限公司、上海牛之云网络科技有限公司、合肥奇乐网络科技有限公司、北京国炬信息技术有限公司、乐至（上海）科技有限公司、上海师廉网络科技发展有限公司、淄博闪灵网络科技有限公司、武汉贝云网络科技有限公司、北京康盛新创科技有限责任公司、山东艾弗信息科技有限公司、深圳市锟锆科技有限公司、沈阳点动科技有限公司、深圳市龙艺脉网络科技有限公司、哈尔滨朗威电子技术开发有限公司、上海叶云网络科技有限公司、深圳市网心科技有限公司、成都康菲顿特网络科技有限公司、长沙友点软件科技有限公司、沧州市凡诺广告传媒有限公司、北京东土科技股份有限公司、首岳资讯网络股份有限公司、上海装盟信息科技有限公司、广东学苑教育发展有限公司、温州龙诚互联科技有限公司、开平市联科网络科技有限公司、江苏易安联网络技术有限公司、石家庄帝易广告有限公司、北京网瑞达科技有限公司、科华恒盛股份有限公司、西安佰联网络技术有限公司、浙江易舸软件有限公司、上海物创信息科技有限公司、济南白菜网络技术有限公司、湖北国昇科技有限公司、深圳市大点科技有限公司、西安昊博智能科技有限公司、常州巨细信息科技有限公司、广州市互诺计算机科技有限公司、北京天融信科技有限公司、湖北诺千金网络科技有限公司、深圳市超时代软件有限公司、维谛技术有限公司、四平市九州易通科技有限公司、漳州盛行网络科技有限公司、商派软件有限公司、四川信任科技有限公司、上海卓岚信息科技有限公司、甲骨文（中国）软件系统有限公司、北京猎豹移动科技有限公司、国药控股云南有限公司、重庆扬浪科技有限责任公司、安徽环美智能科技有限公司、台湾資生網路、阿里巴巴集团安全应急响应中心、新疆维吾尔自治区人民政府办公厅、深圳市齐力成科技合伙企业（有限合伙）、李雷博客、梦想 CMS、鱼跃 CMS、天途 CMS、苹果 CMS、Phpweb、PHPMyWind、ZZCMS、UCMS、MacCMS、UNICOM Global、Jfinal cm、KiteCMS、Zzzcms、115CMS、ShuipFCMS、VMware, Inc.和 ClickHouse。

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、北京神州绿

盟科技有限公司、中国电信集团系统集成有限责任公司、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、山东华鲁科技发展股份有限公司、北京华云安信息技术有限公司、山东新潮信息技术有限公司、河南灵创电子科技有限公司、远江盛邦（北京）网络安全科技股份有限公司、杭州海康威视数字技术股份有限公司、河南信安世纪科技有限公司、安徽长泰信息安全服务有限公司、广西等保安全测评有限公司、山东道普测评技术有限公司、中科华威（北京）信息技术研究院、山东云天安全技术有限公司、星云博创科技有限公司、北京天地和兴科技有限公司、吉林谛听信息技术有限公司、广州安亿信软件科技有限公司、北京长亭科技有限公司、泽鹿安全、上海观安信息技术股份有限公司、北京禹宏信安科技有限公司、南京众智维信息科技有限公司、浙江安腾信息技术有限公司、北京智游网安科技有限公司、北京惠而特科技有限公司、河北千诚电子科技有限公司、上海犀点意象网络科技有限公司、广州弈安信息科技有限公司、平安银河实验室及其他个人白帽子向 CNVD 提交了 4604 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）和上海交大向 CNVD 共享的白帽子报送的 3431 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）	2541	2541
奇安信网神（补天平台）	456	456
上海交大	434	434
哈尔滨安天科技集团股份有限公司	219	0
北京神州绿盟科技有限公司	215	3
中国电信集团系统集成有限责任公司	122	122
华为技术有限公司	113	0
北京天融信网络安全技术有限公司	105	1
深信服科技股份有限公司	89	0
北京启明星辰信息安全技术有限公司	52	0
新华三技术有限公司	46	0
北京数字观星科技有限公司	38	0

北京安信天行科技有限公司	23	23
北京奇虎科技有限公司	19	19
浙江大华技术股份有限公司	5	5
北京知道创宇信息技术股份有限公司	2	0
国瑞数码零点实验室	208	208
山东华鲁科技发展股份有限公司	58	58
北京华云安信息技术有限公司	37	37
杭州迪普科技股份有限公司	32	0
山东新潮信息技术有限公司	30	30
河南灵创电子科技有限公司	23	23
远江盛邦（北京）网络安全科技股份有限公司	22	22
杭州海康威视数字技术股份有限公司	19	19
河南信安世纪科技有限公司	16	16
安徽长泰信息安全服务有限公司	14	14
广西等保安全测评有限公司	14	14
山东道普测评技术有限公司	10	10
中科华威（北京）信息技术研究院	10	10
山东云天安全技术有限公司	9	9
星云博创科技有限公司	9	9
北京天地和兴科技有限公司	8	8
吉林谛听信息技术有限公司	7	7
广州安亿信软件科技有限公司	5	5

国家互联网应急中心	5	5
北京长亭科技有限公司	4	4
泽鹿安全	4	4
上海观安信息技术股份有限公司	4	4
北京禹宏信安科技有限公司	3	3
南京众智维信息科技有限公司	2	2
浙江安腾信息技术有限公司	1	1
北京智游网安科技有限公司	1	1
北京惠而特科技有限公司	1	1
河北千诚电子科技有限公司	1	1
上海犀点意象网络科技有限公司	1	1
广州弈安信息科技有限公司	1	1
平安银河实验室	1	1
CNCERT 天津分中心	17	17
CNCERT 河北分中心	7	7
CNCERT 海南分中心	5	5
CNCERT 宁夏分中心	2	2
CNCERT 浙江分中心	1	1
CNCERT 山西分中心	1	1
CNCERT 贵州分中心	1	1
个人	438	438
报送总计	5511	4604

本周漏洞按类型和厂商统计

本周，CNVD 收录了 673 个漏洞。WEB 应用 388 个，应用程序 173 个，操作系统 62 个，网络设备（交换机、路由器等网络端设备）20 个，数据库 11 个，智能设备（物联网终端设备）漏洞 10 个，安全产品 9 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
WEB 应用	388
应用程序	173
操作系统	62
网络设备（交换机、路由器等网络端设备）	20
数据库	11
智能设备（物联网终端设备）漏洞	10
安全产品	9

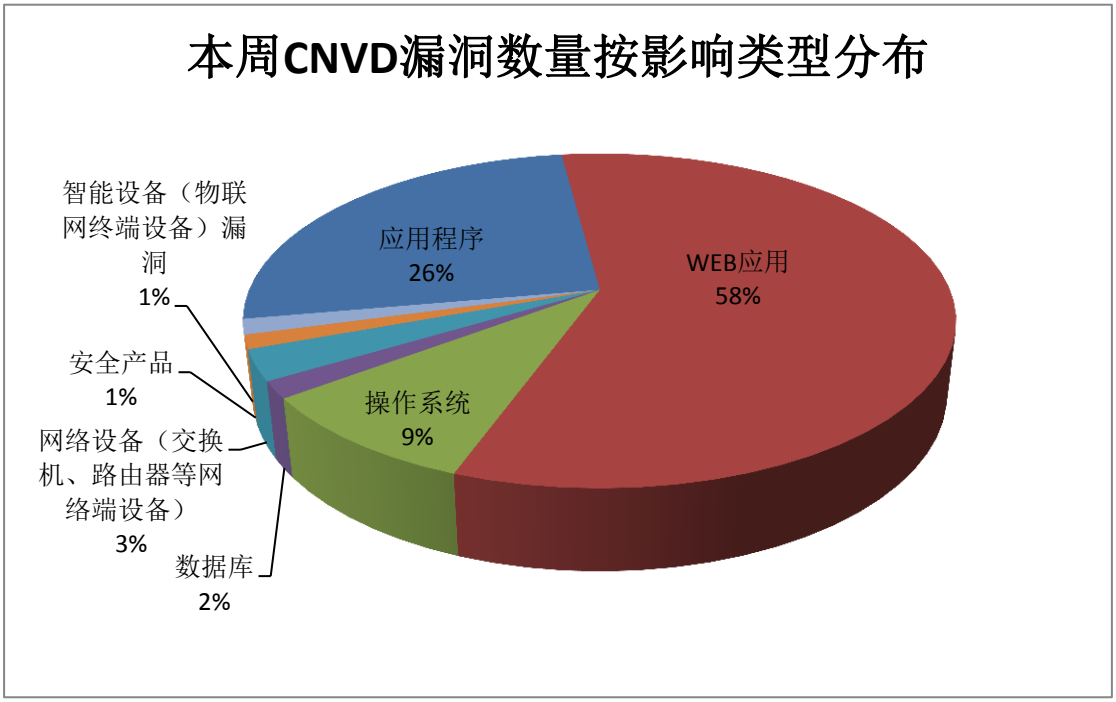

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Microsoft、Cisco、Mattermost 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	41	6%
2	Cisco	20	3%
3	Mattermost	20	3%
4	Apple	26	4%

5	IBM	16	2%
6	Dbhcms	13	2%
7	Sierra Wireless	10	1%
8	研华科技（中国）有限公司	10	1%
9	海南易而优科技有限公司	9	2%
10	其他	508	76%

本周行业漏洞收录情况

本周，CNVD 收录了 19 个电信行业漏洞，43 个移动互联网行业漏洞，24 个工控行业漏洞（如下图所示）。其中，“C-More HMI EA9 访问控制错误漏洞、Billion Smart Energy Router SG600R2 命令执行漏洞、Citrix Systems XenMobile Server 命令注入漏洞、多款 Apple 产品 ImageIO 组件任意代码执行漏洞、Cisco NX-OS Software 命令注入漏洞”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/

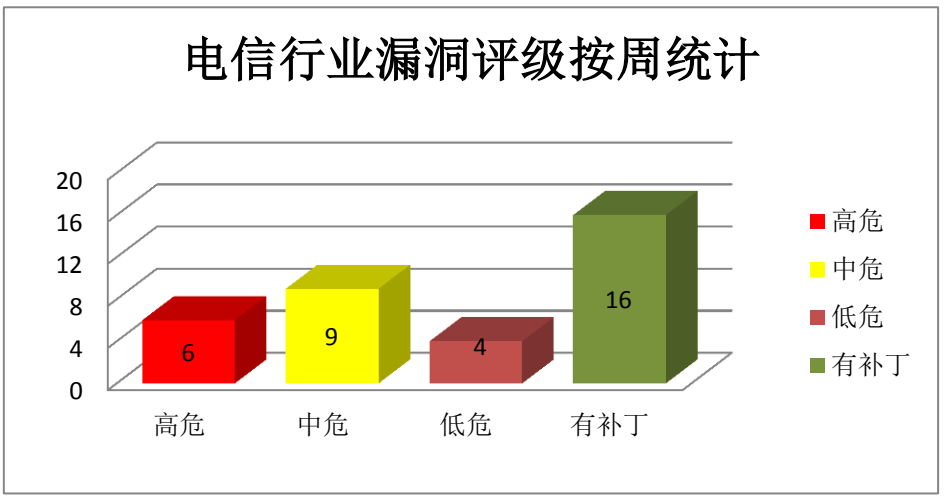

图 3 电信行业漏洞统计

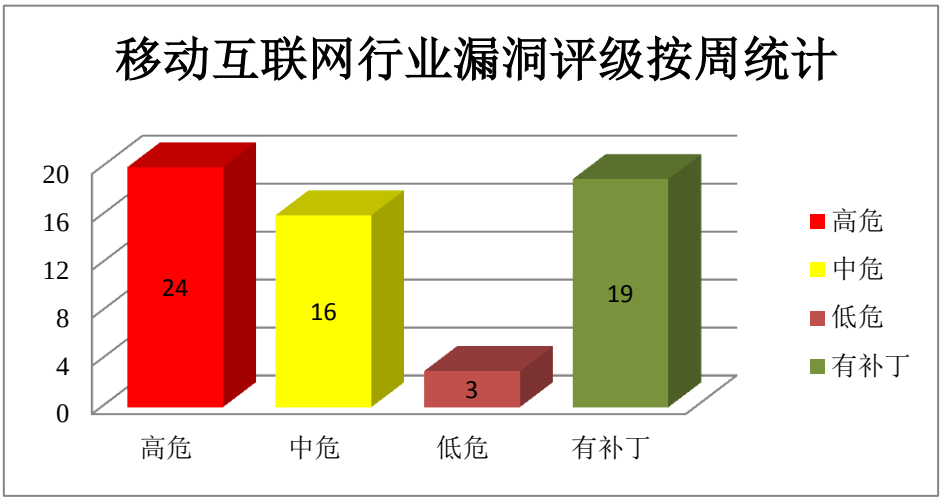

图 4 移动互联网行业漏洞统计

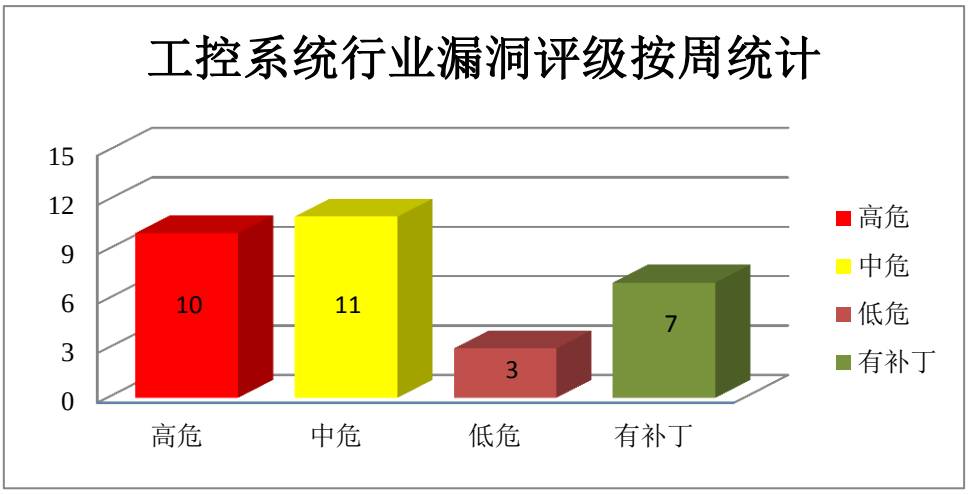

图 5 工控系统行业漏洞统计

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 Internet Explorer（IE）是一款 Windows 操作系统附带的 Web 浏览器。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。Microsoft Excel 是一款 Office 套件中的电子表格处理软件。Microsoft Office 是一款办公软件套件产品。Microsoft SharePoint 是一套企业业务协作平台。Microsoft Word 是一套 Office 套件中的文字处理软件。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞获取敏感信息，提升权限，执行任意代码。

CNVD 收录的相关漏洞包括：Microsoft Internet Explorer 远程代码执行漏洞（CNVD-2020-47963）、Microsoft Windows 和 Microsoft Windows Server 权限提升漏洞（CNVD-2020-48258、CNVD-2020-48261、CNVD-2020-48270、CNVD-2020-48274）、Microso

ft Excel 远程代码执行漏洞（CNVD-2020-48604）、Microsoft Excel 代码执行漏洞（CNVD-2020-48656）、Microsoft Word 信息泄露漏洞（CNVD-2020-49005）。其中，除“Microsoft Word 信息泄露漏洞（CNVD-2020-49005）”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-2020-47963
https://www.cnvd.org.cn/flaw/show/CNVD-2020-48258
https://www.cnvd.org.cn/flaw/show/CNVD-2020-48261
https://www.cnvd.org.cn/flaw/show/CNVD-2020-48270
https://www.cnvd.org.cn/flaw/show/CNVD-2020-48274
https://www.cnvd.org.cn/flaw/show/CNVD-2020-48604
https://www.cnvd.org.cn/flaw/show/CNVD-2020-48656
https://www.cnvd.org.cn/flaw/show/CNVD-2020-49005

2、Cisco 产品安全漏洞

Cisco Nexus 9000 Series Switches 是一款 9000 系列交换机。Cisco Nexus 9500 R-Series Line Cards and Fabric Modules 是一款 9500R 系列线卡模块。Cisco Nexus 3000 Series Switches 是一款 3000 系列交换机。Cisco Nexus 3500 Platform Switches 是一款 3500 系列平台交换机。Cisco NX-OS Software 是一套交换机使用的数据中心级操作系统软件。Cisco Nexus 7000 Series Switches 是一款 7000 系列交换机。Cisco MDS 9000 Series Multilayer Switches 是一款 MDS 9000 系列多层交换机。Cisco Video Surveillance 8000 Series IP Cameras 是一款网络摄像设备。Cisco Small Business Smart and Managed Switches 是一款思科交换机设备。Cisco Data Center Network Manager（DCNM）是一套数据中心管理系统。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞在底层操作系统上以提升的权限执行任意命令，造成拒绝服务等。

CNVD 收录的相关漏洞包括：Cisco Nexus 9000 Series FCoE NPV 拒绝服务漏洞、Cisco NX-OS Software CLI 命令注入漏洞（CNVD-2020-47610）、Cisco NX-OS Software 命令注入漏洞（CNVD-2020-47609、CNVD-2020-47607、CNVD-2020-47611）、Cisco Data Center Network Manager 跨站脚本漏洞（CNVD-2020-48587）、Cisco Video Surveillance 8000 Series IP Cameras 内存泄露漏洞、Cisco Small Business Smart and Managed Switches 拒绝服务漏洞。其中，“Cisco NX-OS Software CLI 命令注入漏洞（CNVD-2020-47610）、Cisco NX-OS Software 命令注入漏洞（CNVD-2020-47609、CNVD-2020-47607、CNVD-2020-47611）”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-2020-47606
https://www.cnvd.org.cn/flaw/show/CNVD-2020-47610

https://www.cnvd.org.cn/flaw/show/CNVD-2020-47609

https://www.cnvd.org.cn/flaw/show/CNVD-2020-47607

https://www.cnvd.org.cn/flaw/show/CNVD-2020-47611

https://www.cnvd.org.cn/flaw/show/CNVD-2020-48587

https://www.cnvd.org.cn/flaw/show/CNVD-2020-48990

https://www.cnvd.org.cn/flaw/show/CNVD-2020-48989

3、IBM 产品安全漏洞

IBM Security Guardium 是一套提供数据保护功能的平台。IBM Verify Gateway（IVG）是一套基于云的身份验证解决方案。IBM QRadar SIEM 是一套利用安全智能保护资产和信息远离高级威胁的解决方案。IBM InfoSphere Information Server 是一套数据整合平台。IBM Spectrum Virtualize 是一款纯软件的存储产品，支持软件定义存储管理和保护海量数据。IBM Planning Analytics 是一套业务规划分析解决方案。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，执行任意代码等。

CNVD 收录的相关漏洞包括：IBM Security Guardium 信息泄露漏洞（CNVD-2020-47942）、IBM Verify Gateway 信息泄露漏洞、IBM QRadar SIEM 跨站脚本漏洞（CNVD-2020-47950）、IBM QRadar SIEM 操作系统命令注入漏洞、IBM InfoSphere Information Server 远程代码执行漏洞、IBM QRadar SIEM XML 实体注入漏洞、IBM Spectrum Virtualize 权限提升漏洞、IBM Planning Analytics Workspace 资源管理错误漏洞。其中，“IBM InfoSphere Information Server 远程代码执行漏洞”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-2020-47942

https://www.cnvd.org.cn/flaw/show/CNVD-2020-47944

https://www.cnvd.org.cn/flaw/show/CNVD-2020-47950

https://www.cnvd.org.cn/flaw/show/CNVD-2020-47948

https://www.cnvd.org.cn/flaw/show/CNVD-2020-47953

https://www.cnvd.org.cn/flaw/show/CNVD-2020-47951

https://www.cnvd.org.cn/flaw/show/CNVD-2020-48601

https://www.cnvd.org.cn/flaw/show/CNVD-2020-49271

4、Apple 产品安全漏洞

Apple macOS Catalina 是一套专为 Mac 计算机所开发的专用操作系统。Apple iOS 是一套为移动设备所开发的操作系统。Apple tvOS 是一套智能电视操作系统。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。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞执行任意代码。

CNVD 收录的相关漏洞包括：Apple macOS Catalina CoreAudio 组件缓冲区溢出漏

洞、多款 Apple 产品 ImageIO 组件任意代码执行漏洞、Apple tvOS、iOS 和 iPadOS AVEVideoEncoder 组件任意代码执行漏洞、多款 Apple 产品 Audio 组件任意代码执行漏洞（CNVD-2020-49300）、Apple iOS、iPadOS 和 watchOS Kernel 组件内存破坏漏洞、Apple macOS Catalina Graphics Drivers 组件越界读取漏洞、Apple macOS Catalina Sandbox 组件命令注入漏洞、Apple macOS Catalina ksh shell 命令执行漏洞。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-2020-49303
https://www.cnvd.org.cn/flaw/show/CNVD-2020-49302
https://www.cnvd.org.cn/flaw/show/CNVD-2020-49301
https://www.cnvd.org.cn/flaw/show/CNVD-2020-49300
https://www.cnvd.org.cn/flaw/show/CNVD-2020-49304
https://www.cnvd.org.cn/flaw/show/CNVD-2020-49315
https://www.cnvd.org.cn/flaw/show/CNVD-2020-49313
https://www.cnvd.org.cn/flaw/show/CNVD-2020-49317

5、Silicon Labs Bluetooth Low Energy SDK 缓冲区溢出漏洞

Silicon Labs Bluetooth Low Energy SDK 是一款低功能蓝牙开发套件。本周，Silicon Labs Bluetooth Low Energy SDK 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，使应用程序崩溃或在应用程序上下文执行任意代码。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-2020-48988

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-2020-47962	PHP 资源管理错误漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://bugs.php.net/bug.php?id=79797
CNVD-2020-47961	Micro Air Vehicle Link 路径遍历漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://mavlink.io/
CNVD-2020-48577	FasterXML jackson-databind 反序列化漏洞	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/issues/2814
CNVD-2020-48582	Squid 拒绝服务漏洞（CNVD-2020-48582）	高	厂商已发布了漏洞修复程序，请及时关注更新：

			https://github.com/squid-cache/squid/security/advisories/GHSA-vvj7-xjgq-g2jg
CNVD-2020-49028	Citrix Systems XenMobile Server 命令注入漏洞	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.citrix.com/article/CTX277457
CNVD-2020-49036	Juniper Networks Junos OS 拒绝服务漏洞（CNVD-2020-49036）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11031
CNVD-2020-49043	C-MORE HMI EA9 访问控制错误漏洞（CNVD-2020-49043）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.automationdirect.com/
CNVD-2020-49041	Veeam ONE XML 外部实体引用漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.veeam.com/kb3221
CNVD-2020-49264	QEMU 输入验证错误漏洞（CNVD-2020-49264）	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.qemu.org/
CNVD-2020-49267	RangeeOS OS 命令注入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://rangee.com/en/rangee-os/

小结：本周，Microsoft 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。此外，Cisco、IBM、Apple 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，造成拒绝服务等。另外，Silicon Labs Bluetooth Low Energy SDK 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，使应用程序崩溃或在应用程序上下文执行任意代码。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、LimeSurvey 'Survey Menu'存储型跨站脚本漏洞

验证描述

LimeSurvey（前称 PHPSurveyor）是 LimeSurvey 团队的一套开源的在线问卷调查程序，它支持调查程序开发、调查问卷发布以及数据收集等功能。

LimeSurvey 'Survey Menu'存在存储型跨站脚本漏洞。攻击者可利用漏洞获取用户 cookie 等敏感信息。

验证信息

POC 链接：https://www.exploitalert.com/view-details.html?id=36030

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2020-48579

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. 宝塔面板曝出严重安全漏洞，尽快升级到最新版本

宝塔面板被曝出存在严重安全漏洞，目前官方已经给宝塔面板用户发送短信提醒升级，影响范围包括了宝塔 linux 面板 7.4.2 以及宝塔 windows 面板 6.8。

参考链接：https://www.chinaz.com/2020/0824/1175116.shtml

2. 专家揭示了未修复的 Safari 漏洞，该漏洞允许窃取本地文件

一位研究人员披露了苹果 Safari 网络浏览器中未修补漏洞的技术细节，该漏洞可被利用来从目标系统中窃取文件。苹果在 8 月份告诉研究人员，将在 2021 年春季解决该问题，并要求他在此之前不要公开披露该问题。

参考链接：https://securityaffairs.co/wordpress/107507/hacking/apple-safari-browser-flaw.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