国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2021 年 12 月 13 日-2021 年 12 月 19 日　　2021 年第 50 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 620 个，其中高危漏洞 195 个、中危漏洞 351 个、低危漏洞 74 个。漏洞平均分值为 5.75。本周收录的漏洞中，涉及 0day 漏洞 303 个（占 49%），其中互联网上出现“B2evolution 跨站脚本漏洞（CNVD-2021-100271）、ZZCMS SQL 注入漏洞（CNVD-2021-99769）”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 10886 个，与上周（35692 个）环比增加 69%。

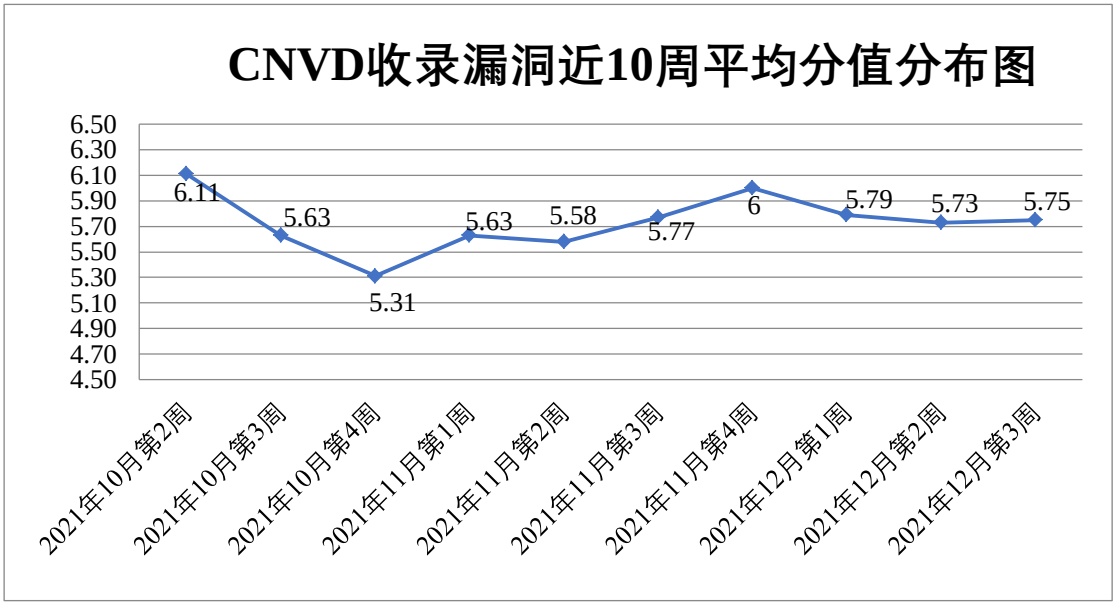

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 25 起，向基础电信企业通报漏洞事件 32 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 585 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 106 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 72 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：

紫光软件系统有限公司、淄博闪灵网络科技有限公司、中国电信集团有限公司、智汇方象（青岛）软件有限公司、浙江中控技术股份有限公司、浙江深大智能科技有限公司、浙江兰德纵横网络技术股份有限公司、浙江标点信息科技有限公司、长沙友点软件科技有限公司、长沙米拓信息技术有限公司、友讯电子设备（上海）有限公司、用友网络科技股份有限公司、兄弟（中国）商业有限公司、新天科技股份有限公司、新都（青岛）电子有限公司、小米科技有限责任公司、西安创富电子科技有限公司、唯栎电子科技（上海）有限公司、微软（中国）有限公司、太原易思软件技术有限公司、苏州思迪信息技术有限公司、松下电器（中国）有限公司、四平市九州易通科技有限公司、思科系统（中国）网络技术有限公司、曙光信息产业股份有限公司、深圳市志华环讯软件科技有限公司、深圳市永泰新欣科技有限公司、深圳市网域科技技术有限公司、深圳市天翼软件有限公司、深圳市腾讯计算机系统有限公司、深圳市商通在线科技有限公司、深圳市龙兄弟数码锁有限公司、深圳市锟铻科技有限公司、深圳市巨龙科教网络有限公司、深圳市吉祥腾达科技有限公司、深圳市惠尔顿信息技术有限公司、深圳市皓峰通讯技术有限公司、深圳齐心好视通云计算有限公司、上海智休信息科技有限公司、上海易教信息科技有限公司、上海焱凤信息技术有限公司、上海华测导航技术股份有限公司、上海恒生聚源数据服务有限公司、上海泛微网络科技股份有限公司、上海顶想信息科技有限公司、上海艾泰科技有限公司、陕西华筑科技有限公司、山石网科通信技术（北京）有限公司、山东思达特测控设备有限公司、山东来客网络科技有限公司、厦门一指通智能科技有限公司、厦门四信通信科技有限公司、瑞斯康达科技发展股份有限公司、青岛东胜伟业软件有限公司、青岛东橙网站建设公司、普联技术有限公司、宁波亿发展电子商务集团有限公司、南京科远智慧科技集团股份有限公司、南昌航天广信科技有限责任公司、摩莎科技（上海）有限公司、零视技术（上海）有限公司、联奕科技股份有限公司、连云港信友科技有限公司、浪潮云信息技术股份公司、昆仑数智科技有限责任公司、金蝶软件（中国）有限公司、焦作市蓝恩网络科技有限公司、江西金磊科技发展有限公司、江西金格科技有限公司、江苏紫清信息科技有限公司、佳能（中国）有限公司、济南安众信息科技有限公司、淮南市银泰软件科技有限公司、湖南建研信息技术股份有限公司、湖北点点点科技有限公司、河北谱云科技有限公司、杭州中宝科技有限公司、杭州易现先进科技有限公司、杭州迪普科技股份有限公司、贵州觅新科技有限公司、广州粤建三和软件股份有限公司、广州同鑫科技有限公司、广州市璐华计算机有限公司、广州市奥威亚电子科技有限公司、广州合优网络科技有限公司、广东凯格科技有限公司、广东飞

企互联科技股份有限公司、富士胶片商业创新（中国）有限公司、福建星网智慧科技有限公司、福建福昕软件开发股份有限公司、戴尔（中国）有限公司、成都索贝数码科技股份有限公司、畅捷通信息技术股份有限公司、北京中科网威信息技术有限公司、北京致远互联软件股份有限公司、北京英华在线科技有限公司、北京星网锐捷网络技术有限公司、北京通达信科科技有限公司、北京天星组态软件有限公司、北京数科网维技术有限责任公司、北京派网软件有限公司、北京旷视科技有限公司、北京酷我科技有限公司、北京京视健康科技有限公司、北京慧图科技（集团）股份有限公司、北京当当科文电子商务有限公司、北京博海琪林科技有限公司、北京北森云计算股份有限公司、保定飞凌嵌入式技术有限公司、安徽旭帆信息科技有限公司、安徽听见科技有限公司、安徽青柿信息科技有限公司、安徽彩屋教育科技有限公司、阿里巴巴集团安全应急响应中心、上海布雷德网络科技、北京科技大学计算机与通信工程学院、信呼、熊海 CMS、小说精品屋、梦想 CMS、ZKBH2021、Yamaha Corporation、uchat 智优客服、TRENDnet、TOTOLINK、The Apache Software Foundation、Sapido Technology Inc、Rockwell Automation、Kyan、JeePlus、IObit、emlog、DWG TOOL Software、Catfish CMS 和 Adobe。

本周，CNVD 发布了《关于 Apache Log4j2 存在远程代码执行漏洞的安全公告（第二版）》、《Apache Log4j2 远程代码执行漏洞排查及修复手册》、《Microsoft 发布 2021 年 12 月安全更新》。详情参见 CNVD 网站公告内容。

https://www.cnvd.org.cn/webinfo/show/7121

https://www.cnvd.org.cn/webinfo/show/7146

https://www.cnvd.org.cn/webinfo/show/7151

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、哈尔滨安天科技集团股份有限公司、新华三技术有限公司、北京神州绿盟科技有限公司、恒安嘉新（北京）科技股份公司等单位报送公开收集的漏洞数量较多。北京信联科汇科技有限公司、广东蓝爵网络安全技术股份有限公司、北京云科安信科技有限公司（Seraph 安全实验室）、贵州多彩宝互联网服务有限公司、河南灵创电子科技有限公司、南京众智维信息科技有限公司、北京华云安信息技术有限公司、安徽长泰科技有限公司、山东新潮信息技术有限公司、京东云安全、北京安帝科技有限公司、内蒙古洞明科技有限公司、福建省海峡信息技术有限公司、杭州海康威视数字技术股份有限公司、杭州迪普科技股份有限公司、华鲁数智信息技术（北京）有限公司、快页信息技术有限公司、重庆都会信息科技有限公司、上海纽盾科技股份有限公司、杭州天谷信息科技有限公司、思而听网络科技有限公司、广州安亿信软件科技有限公司、杭州美创科技有限公司、广州易东信息安全技术有限公司、河南信安世纪科技有限公司、山石网科通信技术股份有限公司、

北京墨云科技有限公司、平安银河实验室、北京机沃科技有限公司、上海计算机软件技术开发中心、中移（杭州）信息技术有限公司、北京未来智安科技有限公司、中孚信息股份有限公司、智网安云（武汉）信息技术有限公司、山东云天安全技术有限公司、广州百蕴启辰科技有限公司、浙江木链物联网科技有限公司、深圳市魔方安全科技有限公司、博智安全科技股份有限公司、及其他个人白帽子向 CNVD 提交了 10886 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、北京鸿腾智能科技有限公司和奇安信网神（补天平台）向 CNVD 共享的白帽子报送的 8924 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
奇安信网神（补天平台）	5311	5311
斗象科技（漏洞盒子）	3261	3261
北京天融信网络安全技术有限公司	338	47
北京鸿腾智能科技有限公司	302	302
哈尔滨安天科技集团股份有限公司	274	24
新华三技术有限公司	217	0
北京神州绿盟科技有限公司	182	11
恒安嘉新（北京）科技股份公司	142	0
深信服科技股份有限公司	107	2
北京启明星辰信息安全技术有限公司	68	11
天津市国瑞数码安全系统股份有限公司	59	0
上海交大	50	50
杭州安恒信息技术股份有限公司	29	29
北京数字观星科技有限公司	27	0

北京长亭科技有限公司	3	3
北京知道创宇信息技术有限公司	3	1
西安四叶草信息技术有限公司	1	1
北京华顺信安科技有限公司	175	0
北京信联科汇科技有限公司	98	98
中国电信股份有限公司网络安全产品运营中心	81	0
广东蓝爵网络安全技术股份有限公司	58	58
北京云科安信科技有限公司（Seraph 安全实验室）	58	58
贵州多彩宝互联网服务有限公司	22	22
河南灵创电子科技有限公司	57	57
南京众智维信息科技有限公司	48	48
北京华云安信息技术有限公司	46	46
西门子（中国）有限公司	46	0
安徽长泰科技有限公司	41	41
山东新潮信息技术有限公司	38	38
京东云安全	25	25
北京安帝科技有限公司	22	22

内蒙古洞明科技有限公司	21	21
福建省海峡信息技术有限公司	20	20
杭州海康威视数字技术股份有限公司	19	19
杭州迪普科技股份有限公司	17	2
华鲁数智信息技术（北京）有限公司	8	8
快页信息技术有限公司	7	7
重庆都会信息科技有限公司	5	5
上海纽盾科技股份有限公司	4	4
杭州天谷信息科技有限公司	4	4
思而听网络科技有限公司	4	4
广州安亿信软件科技有限公司	3	3
杭州美创科技有限公司	2	2
广州易东信息安全技术有限公司	2	2
河南信安世纪科技有限公司	2	2
山石网科通信技术股份有限公司	2	2
北京墨云科技有限公司	1	1
平安银河实验室	1	1
北京机沃科技有限公司	1	1

上海计算机软件技术开发中心	1	1
中移（杭州）信息技术有限公司	1	1
北京未来智安科技有限公司	1	1
中孚信息股份有限公司	1	1
智网安云（武汉）信息技术有限公司	1	1
山东云天安全技术有限公司	1	1
广州百蕴启辰科技有限公司	1	1
浙江木链物联网科技有限公司	1	1
深圳市魔方安全科技有限公司	1	1
博智安全科技股份有限公司	1	1
CNCERT 四川分中心	2	2
个人	1202	1200
报送总计	12526	10886

本周漏洞按类型和厂商统计

本周，CNVD 收录了 620 个漏洞。WEB 应用 284 个，应用程序 204 个，网络设备（交换机、路由器等网络端设备）46 个，操作系统 45 个，智能设备（物联网终端设备）23 个，安全产品 13 个，数据库 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
WEB 应用	284
应用程序	204
网络设备（交换机、路由器等网络端设备）	46
操作系统	45

智能设备（物联网终端设备）	23
安全产品	13
数据库	5

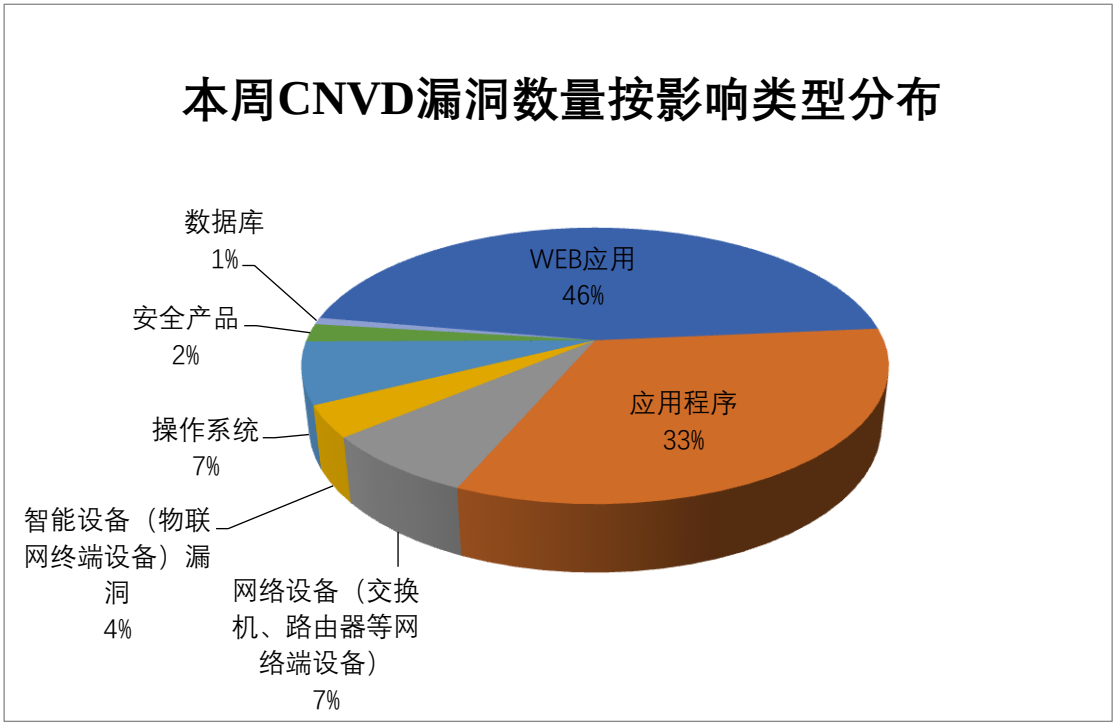

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Huawei、WordPress、SIEMENS 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	Huawei	40	6%
2	WordPress	32	5%
3	SIEMENS	29	5%
4	淄博闪灵网络科技有限公司	25	4%
5	Google	18	3%
6	SourceCodester	16	3%
7	IBM	14	2%
8	mozilla	12	2%
9	Discourse	12	2%
10	其他	422	68%

本周行业漏洞收录情况

本周，CNVD 收录了 14 个电信行业漏洞，13 个移动互联网行业漏洞，9 个工控行

业漏洞（如下图所示）。其中，“Dell Networking OS10 身份验证绕过漏洞（CNVD-2021-99661）、SiPass integrated 访问控制漏洞”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/

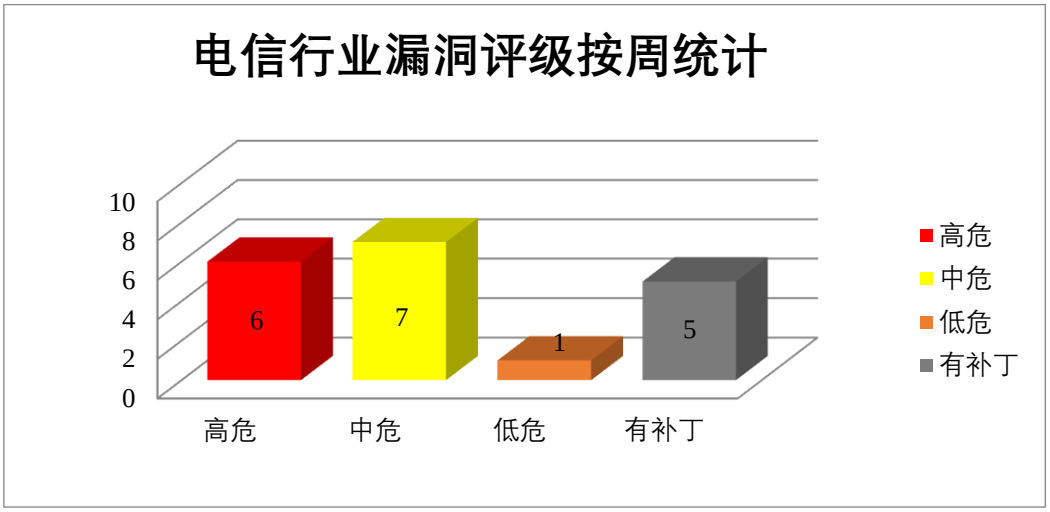

图 3 电信行业漏洞统计

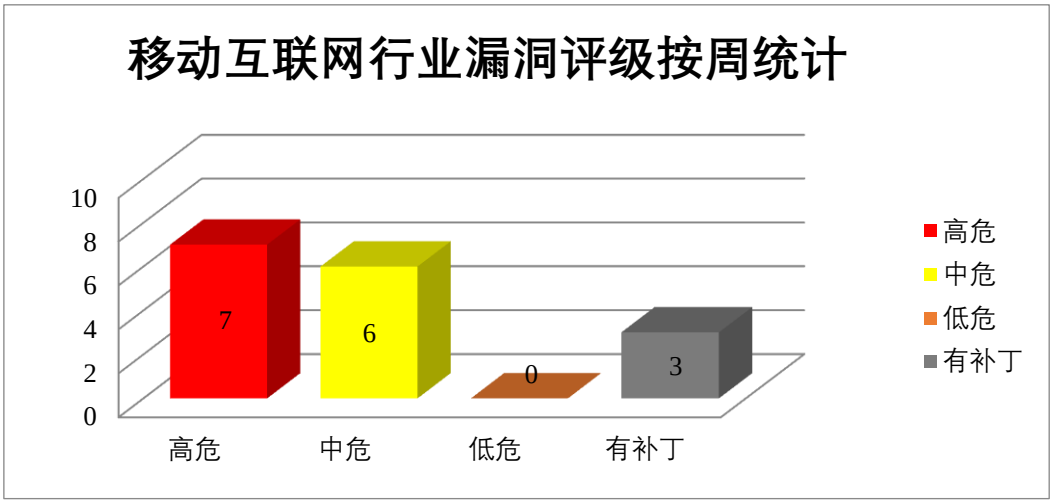

图 4 移动互联网行业漏洞统计

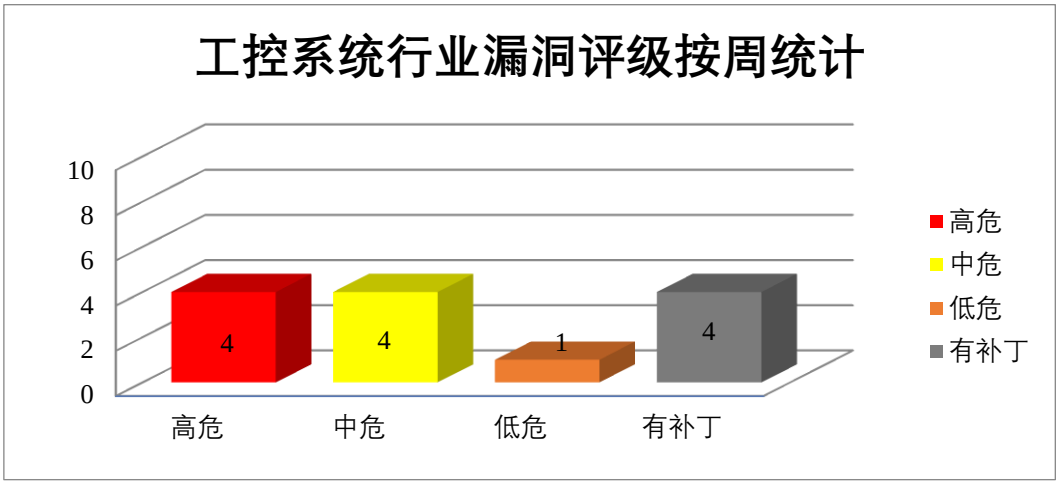

图 5 工控系统行业漏洞统计

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、Huawei 产品安全漏洞

Huawei HarmonyOS 是中国华为（Huawei）公司的一个操作系统。提供一个基于微内核的全场景分布式操作系统。Huawei Emui 是一款基于 Android 开发的移动端操作系统。Magic Ui 是一款基于 Android 开发的移动端操作系统。本周，上述产品被披露存在多个漏洞，攻击者可利用该漏洞导致越界读取，内核崩溃，设备重启等。

CNVD 收录的相关漏洞包括：Huawei HarmonyOS 堆栈缓冲区溢出漏洞、Huawei HarmonyOS 输入验证错误漏洞（CNVD-2021-99974、CNVD-2021-99973、CNVD-2021-99977、CNVD-2021-99978、CNVD-2021-99981）、Huawei HarmonyOS 分布式文件组件空指针访问漏洞、Huawei Emui 和 Magic UI 编解码器检测模块内存泄露漏洞。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-2021-99969

https://www.cnvd.org.cn/flaw/show/CNVD-2021-99974

https://www.cnvd.org.cn/flaw/show/CNVD-2021-99973

https://www.cnvd.org.cn/flaw/show/CNVD-2021-99977

https://www.cnvd.org.cn/flaw/show/CNVD-2021-99978

https://www.cnvd.org.cn/flaw/show/CNVD-2021-99981

https://www.cnvd.org.cn/flaw/show/CNVD-2021-100642

https://www.cnvd.org.cn/flaw/show/CNVD-2021-100640

2、Mozilla 产品安全漏洞

Mozilla Firefox 是美国 Mozilla 基金会的一款开源 Web 浏览器。本周，上述产品被

披露存在多个漏洞，攻击者可利用该漏洞通过探测加载外部协议的错误消息来识别已安装的应用程序，重定向 URL 到恶意网站，导致缓冲区溢出等。

CNVD 收录的相关漏洞包括：Mozilla Firefox 信息泄露漏洞（CNVD-2021-99616）、Mozilla Firefox 跨站脚本漏洞（CNVD-2021-99615、CNVD-2021-99622）、Mozilla Firefox 资源管理错误漏洞（CNVD-2021-99619）、Mozilla Firefox 条件竞争问题漏洞、Mozilla Firefox 缓冲区溢出漏洞（CNVD-2021-99625）、Mozilla Firefox 输入验证错误漏洞（CNVD-2021-99624）、Mozilla Firefox 访问控制错误漏洞（CNVD-2021-99623）。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-2021-99616
https://www.cnvd.org.cn/flaw/show/CNVD-2021-99615
https://www.cnvd.org.cn/flaw/show/CNVD-2021-99619
https://www.cnvd.org.cn/flaw/show/CNVD-2021-99618
https://www.cnvd.org.cn/flaw/show/CNVD-2021-99622
https://www.cnvd.org.cn/flaw/show/CNVD-2021-99625
https://www.cnvd.org.cn/flaw/show/CNVD-2021-99624
https://www.cnvd.org.cn/flaw/show/CNVD-2021-99623

3、Google 产品安全漏洞

Google Chrome 是美国谷歌（Google）公司的一款 Web 浏览器。Google Android 是美国谷歌（Google）公司的的一套以 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，执行任意代码，导致拒绝服务等。

CNVD 收录的相关漏洞包括：Google Chrome Swiftshader 缓冲区溢出漏洞（CNVD-2021-100599）、Google Chrome file API 代码执行漏洞、Google Chrome Swiftshader 代码执行漏洞（CNVD-2021-100601）、Google Chrome ANGLE 安全绕过漏洞、Google Android 权限提升漏洞（CNVD-2021-100605、CNVD-2021-100604）、Google Chrome autofill 安全绕过漏洞（CNVD-2021-100607）、Google Chrome extensions 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-2021-100599
https://www.cnvd.org.cn/flaw/show/CNVD-2021-100603
https://www.cnvd.org.cn/flaw/show/CNVD-2021-100601
https://www.cnvd.org.cn/flaw/show/CNVD-2021-100600
https://www.cnvd.org.cn/flaw/show/CNVD-2021-100605
https://www.cnvd.org.cn/flaw/show/CNVD-2021-100604
https://www.cnvd.org.cn/flaw/show/CNVD-2021-100607

https://www.cnvd.org.cn/flaw/show/CNVD-2021-100606

4、IBM 产品安全漏洞

IBM Spectrum Copy Data Management 是美国国际商业机器公司（IBM）的实现数据中心副本管理流程的现代化、简化和自动化。IBM DB2 是一套关系型数据库管理系统。IBM Cloud Pak for Security(CP4S)是一个开放式安全平台，可连接到您的现有数据源，生成更深入的洞察，并使您能够利用自动化功能更快采取行动。IBM WebSpher e Application Server 是一款应用服务器产品。该产品是 JavaEE 和 Web 服务应用程序的平台，也是 IBMWebSphere 软件平台的基础。Jazz 是 IBM Rational 面向软件交付技术的下一代协作平台。本周，上述产品被披露存在多个漏洞，攻击者可利用该漏洞泄露敏感信息或消耗内存资源，访问其他数据库并读取或修改文件等。

CNVD 收录的相关漏洞包括：IBM Spectrum Copy Data Management 加密问题漏洞、IBM DB2 信息泄露漏洞（CNVD-2021-99669）、IBM Cloud Pak for Security 授权问题漏洞、IBM Db2 权限提升漏洞（CNVD-2021-99672）、IBM Db2 访问控制错误漏洞、IBM WebSphere Application Server 拒绝服务漏洞（CNVD-2021-99670）、IBM Ja zz for Service Management 跨站脚本漏洞（CNVD-2021-99676）、IBM Jazz for Servic e Management XML 外部实体注入漏洞。其中，“IBM Cloud Pak for Security 授权问题漏洞、IBM Db2 访问控制错误漏洞、IBM WebSphere Application Server 拒绝服务漏洞（CNVD-2021-99670）”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-2021-99663

https://www.cnvd.org.cn/flaw/show/CNVD-2021-99669

https://www.cnvd.org.cn/flaw/show/CNVD-2021-99673

https://www.cnvd.org.cn/flaw/show/CNVD-2021-99672

https://www.cnvd.org.cn/flaw/show/CNVD-2021-99671

https://www.cnvd.org.cn/flaw/show/CNVD-2021-99670

https://www.cnvd.org.cn/flaw/show/CNVD-2021-99676

https://www.cnvd.org.cn/flaw/show/CNVD-2021-99678

5、Amazon WorkSpaces 缓冲区溢出漏洞

Amazon WorkSpaces 是美国亚马逊（Amazon）公司的一种完全托管的持久桌面虚拟化服务，可让您的用户随时随地通过任何受支持的设备访问他们需要的数据、应用程序和资源。本周，Amazon WorkSpaces 被披露存在缓冲区溢出漏洞。攻击者可利用该漏洞在内核模式下执行任意代码或通过特制的 I/O 请求数据包导致拒绝服务。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-2021-100332

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-2021-100340	Accops HyWorks 缓冲区溢出漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.sentinelone.com/labs/usb-over-ethernet-multiple-privilege-escalation-vulnerabilities-in-aws-and-other-major-cloud-services/
CNVD-2021-100347	Gryphon Tower 命令注入漏洞（CNVD-2021-100347）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.tenable.com/security/research/tra-2021-51
CNVD-2021-100363	JT2Go 和 Teamcenter Visualization 文件解析漏洞（CNVD-2021-100363）	高	厂商已提供漏洞修补方案，请关注厂商主页及时更新：https://cert-portal.siemens.com/productcert/pdf/ssa-595101.pdf
CNVD-2021-99645	Sourcecodester Online Learning System 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.sourcecodester.com/
CNVD-2021-99647	Sourcecodester Simple Subscription Website 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://github.com/Dir0x/CVE-2021-43140
CNVD-2021-99646	Sourcecodester Customer Relationship Management System 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.sourcecodester.com/php/14794/customer-relationship-management-crm-system-php-source-code.html。
CNVD-2021-99650	Sourcecodester Engineers Online Portal SQL 注入漏洞（CNVD-2021-99650）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.sourcecodester.com/php/13115/engineers-online-portal-php.html
CNVD-2021-99762	Fortinet Meru AP 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：https://www.fortiguard.com/psirt/FG-IR-21-004
CNVD-2021-99770	Fortinet FortiWeb 命令注入漏洞（CNVD-2021-99770）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://fortiguard.com/advisory/FG-I

			R-21-157
CNVD-2021-99870	WordPress WP Data Access 插件 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://wpscan.com/vulnerability/a9073616-ffd6-4956-b2e7-0fb2eac6e9b5

小结：本周，Huawei 产品被披露存在多个漏洞，攻击者可利用该漏洞导致越界读取，内核崩溃，设备重启等。此外，Mozilla、Google、IBM 等多款产品被披露存在多个漏洞，攻击者可利用该漏洞泄露敏感信息，提升权限，执行任意代码，导致拒绝服务，缓冲区溢出等。另外，Amazon WorkSpaces 被披露存在缓冲区溢出漏洞。攻击者可利用该漏洞在内核模式下执行任意代码或通过特制的 I/O 请求数据包导致拒绝服务。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、ZZCMS SQL 注入漏洞（CNVD-2021-99769）

验证描述

zzcms 是一款集成了前端页面、自定义模板、支付等多功能 cms 系统，使用 php+mysql 的 b/s 结构。采用 mvc 模式方便快速搭建系统。

zzcms 在 8.2 和 8.3 版本中存在 SQL 漏洞，该漏洞与受影响版本未正确过滤用户输入有关。在 dl/dl_print.php 中注册普通用户时存在 SQL 注入漏洞，攻击者可利用该漏洞执行恶意脚本。

验证信息

POC 链接：https://gist.github.com/aaaahuia/583b062b686cdff27554e3c6fa5ac94e

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2021-99769

信息提供者

杭州迪普科技股份有限公司

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. Log4Shell 漏洞公开披露前，至少已在“在野”9 天

Log4j 库中的 Log4Shell 漏洞公开披露前，至少已经被攻击利用了一周之多。

参考链接： https://www.freebuf.com/news/310108.html

2. 中消协测评 50 款 App 发现其中 20 款存不同程度账号注销问题

在是否可以顺利注销 APP 账号方面，50 款 APP 中有 20 款 APP 存在不同程度问题，占总排查比例的 40%。

参考链接：https://www.cnbeta.com/articles/tech/1214407.htm

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