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 20 日-2021 年 12 月 26 日　　2021 年第 51 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 588 个，其中高危漏洞 203 个、中危漏洞 303 个、低危漏洞 82 个。漏洞平均分值为 5.70。本周收录的漏洞中，涉及 0day 漏洞 193 个（占 33%），其中互联网上出现“News Portal Project SQL 注入漏洞（CNVD-2021-102010）、Belloo SQL 注入漏洞”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 19707 个，与上周（10886 个）环比增加 81%。

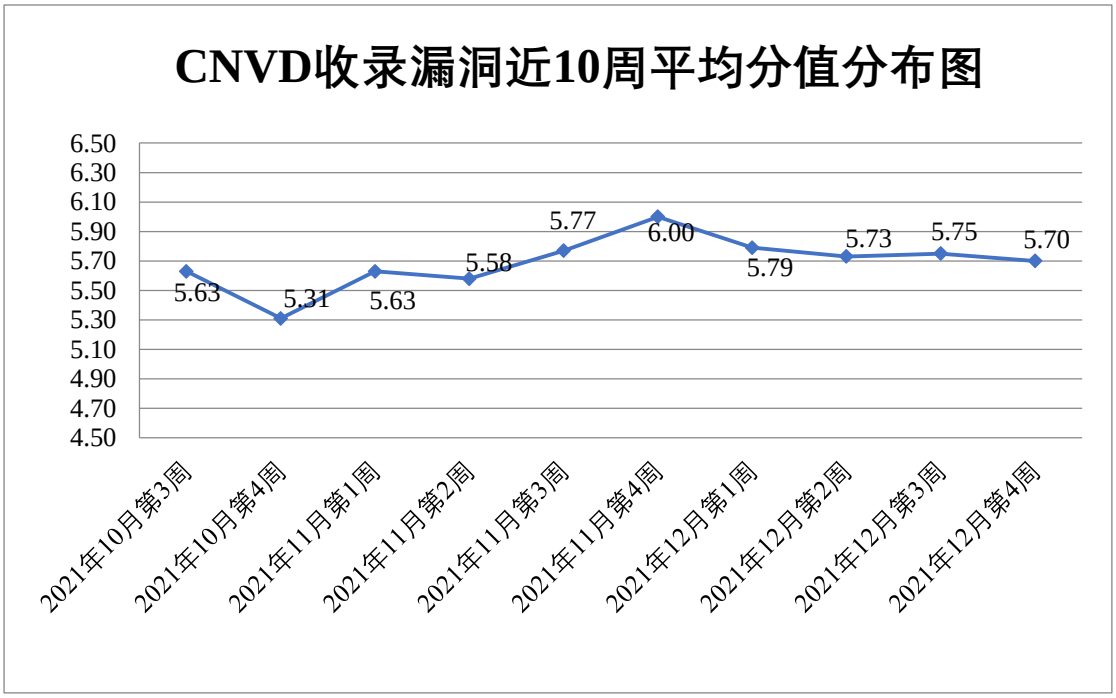

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 23 起，向基础电

信企业通报漏洞事件 17 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 658 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 212 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 51 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：

中兴通讯股份有限公司、中唐方德科技有限公司、中科博华信息科技有限公司、郑州卡卡罗特软件科技有限公司、浙江中控技术股份有限公司、浙江华途信息安全技术股份有限公司、友讯电子设备（上海）有限公司、用友网络科技股份有限公司、易赴科技（集团）有限公司、宜兴易发网络服务有限公司、兄弟（中国）商业有限公司、新天科技股份有限公司、小米科技有限责任公司、西安交大捷普网络科技有限公司、武汉金同方科技有限公司、潍坊家园驿站电子技术有限公司、微软（中国）有限公司、网宿科技股份有限公司、网件（北京）网络技术有限公司、天津天堰科技股份有限公司、四创科技有限公司、四川明腾信息技术有限公司、思科系统（中国）网络技术有限公司、深圳市拓普威视科技有限公司、深圳市前海亿车科技有限公司、深圳市明源云科技有限公司、深圳市捷顺科技实业股份有限公司、深圳市吉祥腾达科技有限公司、深圳市博思协创网络科技有限公司、申瓯通信设备有限公司、上海金慧软件有限公司、上海斐讯数据通信技术有限公司、上海泛微网络科技股份有限公司、上海贝锐信息科技股份有限公司、山东潍微科技股份有限公司、山东金钟科技集团股份有限公司、厦门四信通信科技有限公司、三星（中国）投资有限公司、润申信息科技（上海）有限公司、青岛聚城网络科技有限公司、青岛东胜伟业软件有限公司、普联技术有限公司、尼康映像仪器销售(中国)有限公司、南京悠珀网络科技有限公司、南昌市驰硕网络科技有限公司、明镜远大网络安全信息技术有限公司、美图公司、洛阳市恒凯信息科技有限公司、零视技术（上海）有限公司、联奕科技股份有限公司、朗坤智慧科技股份有限公司、廊坊市极致网络科技有限公司、江西铭软科技有限公司、江苏健科软件有限公司、佳能（中国）有限公司、吉翁电子（深圳）有限公司、湖南青果软件有限公司、湖南竞网智赢网络技术有限公司、衡水迅驰互联网信息服务有限公司、浩通国际货运代理有限公司、杭州映云科技有限公司、杭州荷花软件有限公司、哈尔滨伟成科技有限公司、广州同鑫科技有限公司、广州市奥威亚电子科技有限公司、广州津虹网络传媒有限公司、广州宝露软件开发有限公司、广东精工智能系统有限公司、福建四创软件有限公司、福建科立讯通信有限公司、福建福昕软件开发股份有限公司、成都万江港利科技有限公司、成都三以科技有限公司、北京智邦国际软件技术有限公司、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、北京神州数码云科信息技术有限公司 、北京山石网科信息技术有限公司、北京青云科技股份有限公司、北京卡路里科技有限公司、北京九思协同软件有限公司、北京金和网络股份有限公司、北京高速波软件有限公司、北京东华原医疗设备有限责任公

司、北京百卓网络技术有限公司、北京百容千域软件技术开发有限责任公司、安徽旭帆信息科技有限公司、安徽彩屋教育科技有限公司、腾讯安全应急响应中心、站帮主 CMS、巡云轻论坛系统、熊海 CMS、若依管理系统、梦想 CMS、京瓷集团、帝国软件、Zyxel、x6cms、WordPress、VMware, Inc.、The Apache Software Foundation、TaoCMS、Sapido Technology Inc、mobotix、Jpress、FlexWATCH、emlog、DWG TOOL Software、ClassCMS、BlueCMS 和 Adobe。

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、北京天融信网络安全技术有限公司、西安四叶草信息技术有限公司、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。快页信息技术有限公司、河南灵创电子科技有限公司、广东蓝爵网络安全技术股份有限公司、南京众智维信息科技有限公司、重庆都会信息科技、北京信联科汇科技有限公司、北京山石网科信息技术有限公司、新疆海狼科技有限公司、内蒙古洞明科技有限公司、贵州多彩宝互联网服务有限公司、北京云科安信科技有限公司（Seraph 安全实验室）、西安交大捷普网络科技有限公司、杭州默安科技有限公司、思而听网络科技有限公司、上讯信息、南京树安信息技术有限公司、河南信安世纪科技有限公司、思而听网络科技有限公司、北京百度网讯科技有限公司、福建省海峡信息技术有限公司、北京惠而特科技有限公司、深圳市魔方安全科技有限公司、中安网盾（广州）信息科技有限公司、平安银河实验室、广州易东信息安全技术有限公司、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、星云博创科技有限公司、中移（杭州）信息技术有限公司、安徽长泰科技有限公司、中能融合智慧科技有限公司、上海软件中心、广东安创信息科技开发有限公司、中国银行、中国工商银行、北京快手科技有限公司、江西省掌控者信息安全技术有限公司及其他个人白帽子向 CNVD 提交了 19707 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）、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 17712 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
斗象科技（漏洞盒子）	9400	9400
奇安信网神（补天平台）	7811	7811
北京鸿腾智能科技有限公司	501	501
哈尔滨安天科技集团	228	0

股份有限公司		
北京天融信网络安全技术有限公司	189	85
西安四叶草信息技术有限公司	128	128
北京神州绿盟科技有限公司	126	9
恒安嘉新（北京）科技股份公司	124	0
新华三技术有限公司	82	0
北京数字观星科技有限公司	75	0
深信服科技股份有限公司	72	0
北京启明星辰信息安全技术有限公司	63	3
天津市国瑞数码安全系统股份有限公司	59	0
杭州安恒信息技术股份有限公司	59	47
深圳市腾讯计算机系统有限公司（玄武实验室）	1	1
北京知道创宇信息技术股份有限公司	1	0
北京华顺信安科技有限公司	190	0
快页信息技术有限公司	112	112
河南灵创电子科技有限公司	89	89
广东蓝爵网络安全技术股份有限公司	66	66
南京众智维信息科技	61	61

有限公司		
重庆都会信息科技	59	59
北京信联科汇科技有限公司	48	48
北京山石网科信息技术有限公司	43	43
新疆海狼科技有限公司	39	39
内蒙古洞明科技有限公司	32	32
贵州多彩宝互联网服务有限公司	13	13
北京云科安信科技有限公司（Seraph 安全实验室）	12	12
西安交大捷普网络科技有限公司	8	8
杭州默安科技有限公司	7	7
思而听网络科技有限公司	5	5
上讯信息	4	4
南京树安信息技术有限公司	4	4
河南信安世纪科技有限公司	4	4
思而听网络科技有限公司	3	3
北京百度网讯科技有限公司	3	3
福建省海峡信息技术有限公司	3	3
北京惠而特科技有限公司	3	3

深圳市魔方安全科技有限公司	3	3
中安网盾（广州）信息科技有限公司	2	2
平安银河实验室	2	2
广州易东信息安全技术有限公司	2	2
广州安亿信软件科技有限公司	2	2
山东云天安全技术有限公司	1	1
星云博创科技有限公司	1	1
中移（杭州）信息技术有限公司	1	1
安徽长泰科技有限公司	1	1
中能融合智慧科技有限公司	1	1
上海软件中心	1	1
广东安创信息科技开发有限公司	1	1
中国银行	1	1
中国工商银行	1	1
北京快手科技有限公司	1	1
江西省掌控者信息安全技术有限公司	1	1
CNCERT 四川分中心	3	3
CNCERT 河北分中心	1	1
个人	1079	1078
报送总计	20832	19707

本周漏洞按类型和厂商统计

本周，CNVD 收录了 588 个漏洞。应用程序 253 个，WEB 应用 199 个，操作系统 57 个，网络设备（交换机、路由器等网络端设备）37 个，智能设备（物联网终端设备）25 个，安全产品 12 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
应用程序	253
WEB 应用	199
操作系统	57
网络设备（交换机、路由器等网络端设备）	37
智能设备（物联网终端设备）	25
安全产品	12
数据库	5

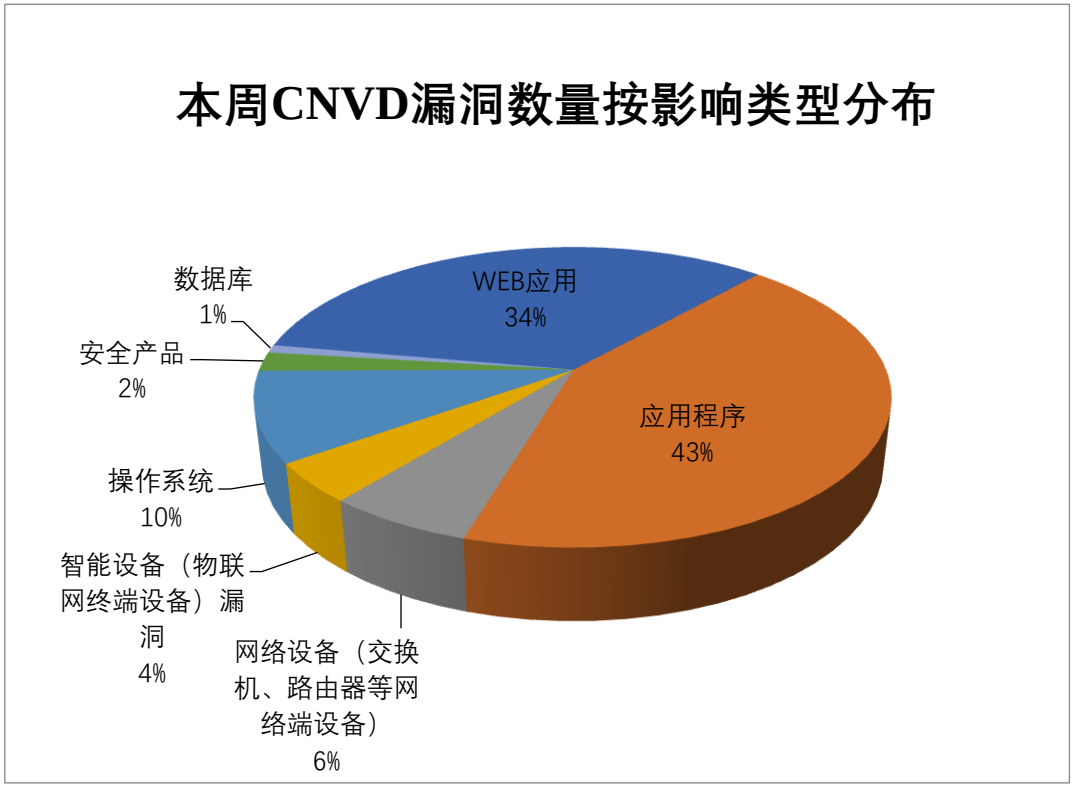

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Bentley Systems、WordPress、Google 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	Bentley Systems	72	12%
2	WordPress	55	9%
3	Google	49	8%
4	Adobe	26	5%

5	Microsoft	16	3%
6	SIEMENS	16	3%
7	Fortinet	15	3%
8	IBM	14	2%
9	淮南市银泰软件科技有限公司	12	2%
10	其他	313	53%

本周行业漏洞收录情况

本周，CNVD 收录了 17 个电信行业漏洞，53 个移动互联网行业漏洞，4 个工控行业漏洞（如下图所示）。其中，“Huawei Cloudengine 5800 权限许可和访问控制问题漏洞、Google Android Media Framework 权限提升漏洞（CNVD-2021-101438）”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/

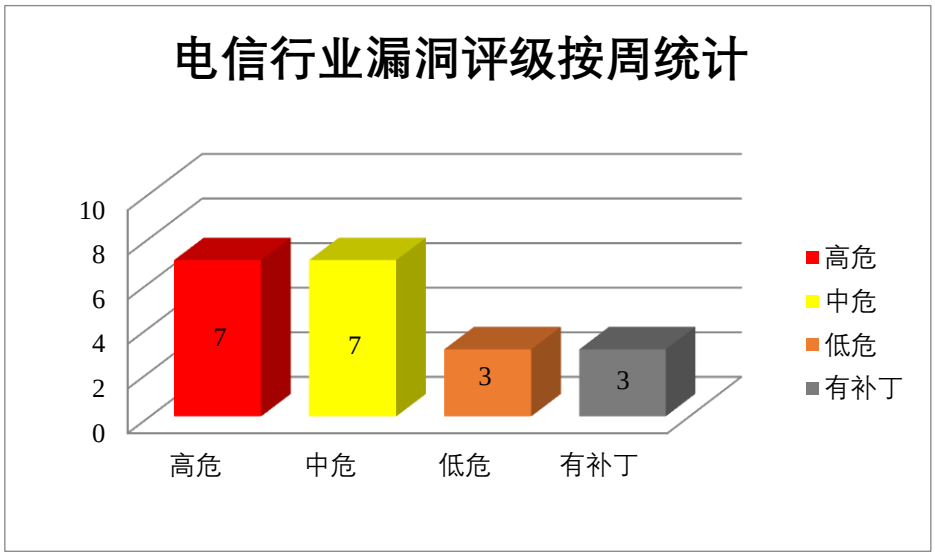

图 3 电信行业漏洞统计

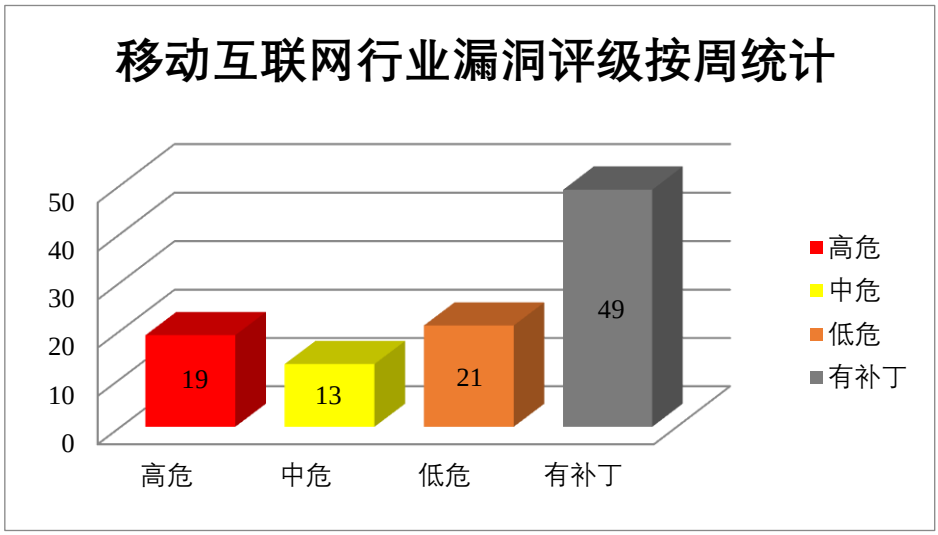

图 4 移动互联网行业漏洞统计

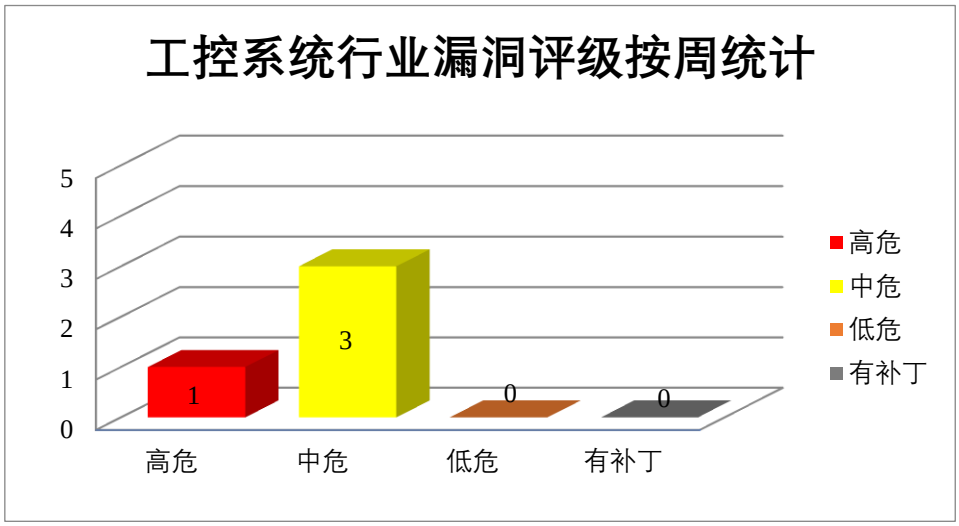

图 5 工控系统行业漏洞统计

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、 Fortinet 产品安全漏洞

Fortinet FortiWeb 是美国飞塔（Fortinet）公司的一款 Web 应用层防火墙。Fortinet FortiOS 是美国飞塔（Fortinet）公司的一套专用于 FortiGate 网络安全平台上的安全操作系统。Fortinet FortiClientEms 是美国 Fortinet 公司的一个集中式中央管理系统。本周，上述产品被披露存在多个漏洞，攻击者可利用该漏洞通过精心设计的 HTTP 请求参数执行未经授权的代码或命令，以明文形式查看敏感信息，将精心构建的 OpenSSL 库放入搜索路径，并以提升的权限在系统上执行任意代码等。

CNVD 收录的相关漏洞包括：Fortinet FortiWeb 命令注入漏洞、Fortinet FortiWeb 跨站脚本漏洞（CNVD-2021-101133）、Fortinet FortiWeb 缓冲区溢出漏洞（CNVD-202

1-101134、CNVD-2021-101138、CNVD-2021-101137）、Fortinet FortiOS 整数溢出漏洞、Fortinet FortiClient 权限提升漏洞（CNVD-2021-102008）、Fortinet FortiClientEms 信息泄露漏洞。其中“Fortinet FortiOS 整数溢出漏洞”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-2021-101131

https://www.cnvd.org.cn/flaw/show/CNVD-2021-101133

https://www.cnvd.org.cn/flaw/show/CNVD-2021-101134

https://www.cnvd.org.cn/flaw/show/CNVD-2021-101138

https://www.cnvd.org.cn/flaw/show/CNVD-2021-101137

https://www.cnvd.org.cn/flaw/show/CNVD-2021-101143

https://www.cnvd.org.cn/flaw/show/CNVD-2021-102008

https://www.cnvd.org.cn/flaw/show/CNVD-2021-102005

2、 Adobe 产品安全漏洞

Adobe Premiere Rush 是美国奥多比（Adobe）公司的一套跨平台的视频编辑软件。本周，上述产品被披露存在代码执行漏洞，攻击者可利用该漏洞在系统上执行任意代码。

CNVD 收录的相关漏洞包括：Adobe Premiere Rush 代码执行漏洞（CNVD-2021-101115、CNVD-2021-101114、CNVD-2021-101117、CNVD-2021-101116、CNVD-2021-101118、CNVD-2021-101120、CNVD-2021-101121、CNVD-2021-101123）。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-2021-101115

https://www.cnvd.org.cn/flaw/show/CNVD-2021-101114

https://www.cnvd.org.cn/flaw/show/CNVD-2021-101117

https://www.cnvd.org.cn/flaw/show/CNVD-2021-101116

https://www.cnvd.org.cn/flaw/show/CNVD-2021-101118

https://www.cnvd.org.cn/flaw/show/CNVD-2021-101120

https://www.cnvd.org.cn/flaw/show/CNVD-2021-101121

https://www.cnvd.org.cn/flaw/show/CNVD-2021-101123

3、 Google 产品安全漏洞

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，攻击者可利用漏洞导致本地权限提升，实现远程代码执行等。

CNVD 收录的相关漏洞包括：Google Android Kernel 组件权限提升漏洞（CNVD-2021-101426、CNVD-2021-101423）、Google Android TvInputManager 组件权限提升漏

洞、Google Android System 权限提升漏洞（CNVD-2021-101432）、Google Android System 远程代码执行漏洞（CNVD-2021-101435、CNVD-2021-101436）、Google Android 越界写入漏洞（CNVD-2021-101951、CNVD-2021-101950）。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-2021-101426
https://www.cnvd.org.cn/flaw/show/CNVD-2021-101424
https://www.cnvd.org.cn/flaw/show/CNVD-2021-101423
https://www.cnvd.org.cn/flaw/show/CNVD-2021-101432
https://www.cnvd.org.cn/flaw/show/CNVD-2021-101435
https://www.cnvd.org.cn/flaw/show/CNVD-2021-101436
https://www.cnvd.org.cn/flaw/show/CNVD-2021-101951
https://www.cnvd.org.cn/flaw/show/CNVD-2021-101950

4、SIEMENS 产品安全漏洞

JT 是由西门子数字工业软件开发的一种公开发布的数据格式。JT Open Toolkit(又称 JTTK)是面向开发人员的应用程序编程接口(API)JT-enabled 软件。JT Open Toolkit 是一个读写工具包。本周，上述产品被披露存在多个漏洞，攻击者可利用该漏洞执行任意代码。

CNVD 收录的相关漏洞包括：JT Utilities 和 JTTK 缓冲区溢出漏洞（CNVD-2021-101000、CNVD-2021-101003）、JT Utilities 和 JTTK 文件解析漏洞（CNVD-2021-101002、CNVD-2021-101005、CNVD-2021-101004、CNVD-2021-101006、CNVD-2021-101008、CNVD-2021-101007）。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-2021-101000
https://www.cnvd.org.cn/flaw/show/CNVD-2021-101002
https://www.cnvd.org.cn/flaw/show/CNVD-2021-101003
https://www.cnvd.org.cn/flaw/show/CNVD-2021-101005
https://www.cnvd.org.cn/flaw/show/CNVD-2021-101004
https://www.cnvd.org.cn/flaw/show/CNVD-2021-101006
https://www.cnvd.org.cn/flaw/show/CNVD-2021-101008
https://www.cnvd.org.cn/flaw/show/CNVD-2021-101007

5、Apache Hadoop Yarn RPC 未授权命令执行漏洞

Apache Hadoop 是一款分布式基础架构。本周，Apache Hadoop Yarn RPC 被披露存在未授权命令执行漏洞。攻击者可利用该漏洞获取服务器控制权限。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-2021-101525

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-2021-101178	jsonpointer 类型混淆漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://snyk.io/vuln/SNYK-JS-JSONPOINTER-1577288
CNVD-2021-101179	Json-Ptr 类型混淆漏洞	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/flitbit/json-ptr/commit/5dc458fbad1c382a2e3ca6d62e66ede3d92849ca
CNVD-2021-101196	VMware vCenter Server 本地提权漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.vmware.com/security/advisories/VMSA-2021-0020.html
CNVD-2021-101199	VMware vCenter Server 文件上传漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.vmware.com/security/advisories/VMSA-2021-0020.html
CNVD-2021-101202	ForgeRock AM 代码问题漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://backstage.forgerock.com/knowledge/kb/article/a47894244
CNVD-2021-101201	ForgeRock AM XML 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://backstage.forgerock.com/knowledge/kb/article/a55763454
CNVD-2021-101200	ForgeRock Access Management 授权问题漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://backstage.forgerock.com/knowledge/kb/article/a55763454
CNVD-2021-101206	OpenMage Magento Lts 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://github.com/OpenMage/magento-lts/security/advisories/GHSA-26rr-v2j2-25fh
CNVD-2021-101217	sgxwallet 缓冲区溢出漏洞（CNVD-2021-101217）	高	厂商已发布了漏洞修复程序，请及时关注更新：

			https://github.com/skalenetwork/sgxwallet/releases
CNVD-2021-101692	iText 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://github.com/itext/itext7/releases/tag/7.1.17

小结：本周， Fortinet 产品被披露存在多个漏洞，攻击者可利用该漏洞通过精心设计的 HTTP 请求参数执行未经授权的代码或命令，以明文形式查看敏感信息，将精心构建的 OpenSSL 库放入搜索路径，并以提升的权限在系统上执行任意代码等。此外，Adobe、Google、SIEMENS 等多款产品被披露存在多个漏洞，攻击者可利用该漏洞在系统上执行任意代码，导致本地权限提升，实现远程代码执行等。另外，Apache Hadoop Yarn RPC 被披露存在未授权命令执行漏洞。攻击者可利用该漏洞获取服务器控制权限。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、Belloo SQL 注入漏洞

验证描述

Belloo 是 Belloo 公司的一个“高质量”的约会软件。

Belloo 存在 SQL 注入漏洞，该漏洞源于 connect.php 中的 ip 参数缺少对外部输入 SQL 语句的验证，攻击者可利用该漏洞执行非法 SQL 命令窃取数据库敏感数据。

验证信息

POC 链接：https://www.chudamax.com/posts/multiple-vulnerabilities-in-belloo-dating-script/

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2021-101949

信息提供者

新华三技术有限公司

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. NVIDIA 已通知客户其产品受 Log4j 缺陷影响

NVIDIA 表示，热门产品，如 GeForce Experience 客户端软件、适用于 Windows

的 GPU 显示驱动程序不在受影响范围内。

参考链接：https://securityaffairs.co/wordpress/125952/security/nvidia-log4shell-impacted-products.html

2. 央视曝光部分 App 禁止全部权限仍可获取用户信息

12 月 25 日，据央视网快看报道，一个移动应用程序安全检测实验室的负责人现场演示了 APP 在后台运行时，是如何窃取用户的个人信息的。

参考链接：https://www.cnbeta.com/articles/tech/1218775.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