国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2021 年 11 月 22 日-2021 年 11 月 28 日　　2021 年第 47 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 643 个，其中高危漏洞 196 个、中危漏洞 411 个、低危漏洞 36 个。漏洞平均分值为 6.0。本周收录的漏洞中，涉及 0day 漏洞 426 个（占 66%），其中互联网上出现“PHP Event Calendar Lite Edition 存在 SQL 注入漏洞、Hitachi Vantara Pentaho 访问控制错误漏洞”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原创漏洞总数 7905 个，与上周（10498 个）环比减少 25%。

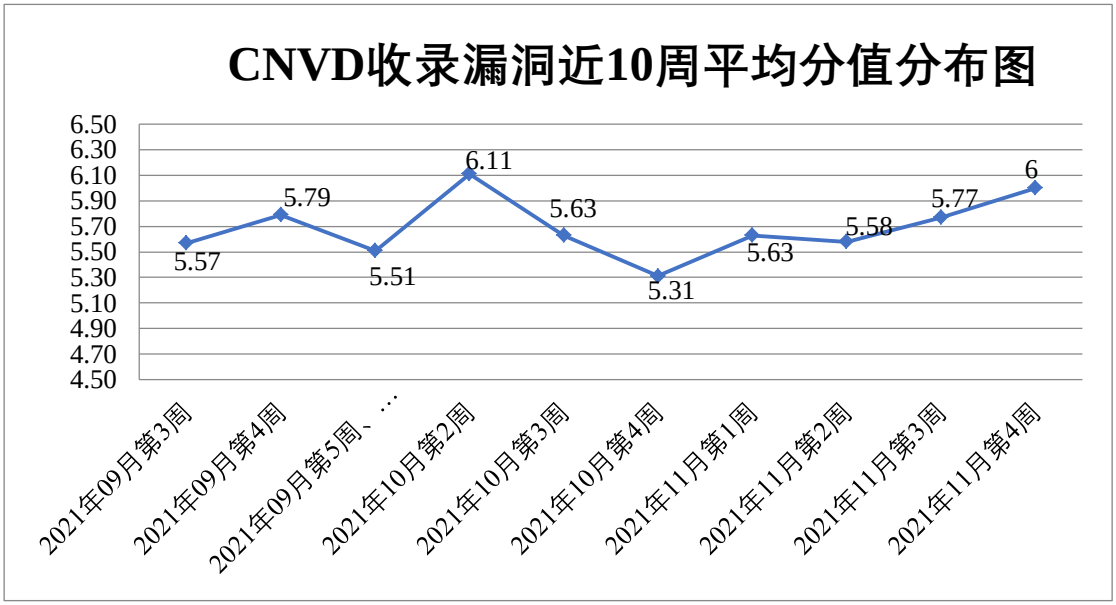

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 34 起，向基础电信企业通报漏洞事件 41 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 548 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 98 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 62 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：

淄博闪灵网络科技有限公司、中科博华信息科技有限公司、中国电信集团有限公司、友讯电子设备（上海）有限公司、用友网络科技股份有限公司、研华科技（中国）有限公司、兄弟（中国）商业有限公司、西安三才科技实业有限公司、微软（中国）有限公司、网通宽带网络有限责任公司、网件（北京）网络技术有限公司、台达电子企业管理(上海)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、四创科技有限公司、世邦通信股份有限公司、深圳维盟科技股份有限公司、深圳市异度信息产业有限公司、深圳市微客互动有限公司、深圳市万网博通科技有限公司、深圳市磊科实业有限公司、深圳市捷视飞通科技股份有限公司、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、深圳市宏电技术股份有限公司、深圳市皓峰通讯技术有限公司、深圳市得伯乐科技有限公司、深圳市朝恒辉网络科技有限公司、深圳市必联电子有限公司、上海卓卓网络科技有限公司、上海小蚁科技有限公司、上海万户信息技术有限公司、上海七十迈数字科技有限公司、上海迈瑞电子科技有限公司、上海华测导航技术股份有限公司、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、上海伯俊软件科技有限公司、上海宝创网络科技有限公司、上海安达通信息安全技术股份有限公司、熵基科技股份有限公司、山西企凝信息科技有限公司、山东思达特测控设备有限公司、厦门石头科技有限公司、三菱电机（中国）有限公司、青岛东软载波科技股份有限公司、普联技术有限公司、鹏博士电信传媒集团股份有限公司、欧普康视科技股份有限公司、欧姆龙自动化（中国）有限公司、南京拓展科技有限公司、南京南软科技有限公司、摩莎科技（上海）有限公司、六安校无忧信息科技有限公司、京瓷办公信息系统(中国)有限公司、金蝶软件（中国）有限公司、杰蛙科技（北京）有限公司、江西铭软科技有限公司、甲骨文股份有限公司、吉翁电子（深圳）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、湖南翱云网络科技有限公司、杭州中宝科技有限公司、杭州伊柯夫科技有限公司、杭州海康威视数字技术股份有限公司、杭州恩软信息技术有限公司、海南有趣科技有限公司、海尔集团电子商务有限公司、哈尔滨新中新电子股份有限公司、桂林崇胜网络科技有限公司、贵州觅新科技有限公司、广州市乐天科技有限公司、广州市保伦电子有限公司、广州迈可硕数据系统有限公司、广东全程云科技有限公司、大唐电信科技股份有限公司、成都青软青之软件有限公司、成都零起飞科技有限公司、成都康菲顿特网络科技有限公司、成都飞鱼星科技股份有限公司、北京中创视讯科技有限公司、北京有孚云计算科技有限公司、北京雪迪龙科技股份有限公司、北京星网锐捷网络技术有限公司、北京速通网电子商务有限公司、北京勤

云科技发展有限公司、北京旷视科技有限公司、北京华医网科技股份有限公司、北京和信创天科技股份有限公司、北京国炬信息技术有限公司、北京百卓网络技术有限公司、奥琦玮信息科技（北京）有限公司、安川電機（中国）有限公司、百度安全应急响应中心、点拓科技、帝国软件、无忧网络、信呼、智睿软件、鱼跃 cms、zzcms、XnSoft、WAVLINK、Trendnet、TOTOLINK、The Apache Software Foundation、TaoCMS、SIKCMS、Rifatron、Handphone 和 Glyph & Cog, LLC。

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，北京神州绿盟科技有限公司、哈尔滨安天科技集团股份有限公司、北京数字观星科技有限公司、新华三技术有限公司、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。贵州多彩宝互联网服务有限公司、杭州迪普科技股份有限公司、山东云天安全技术有限公司、北京信联科汇科技有限公司、杭州海康威视数字技术股份有限公司、北京山石网科信息技术有限公司、河南信安世纪科技有限公司、广东蓝爵网络安全技术股份有限公司、南京树安信息技术有限公司、安徽长泰科技有限公司、长春嘉诚信息技术股份有限公司、中国电信股份有限公司网络安全产品运营中心、京东云安全、北京远禾科技有限公司、北京云科安信科技有限公司（Seraph 安全实验室）、河南灵创电子科技有限公司、北京安帝科技有限公司、山东新潮信息技术有限公司、上海纽盾科技股份有限公司、内蒙古云科数据服务股份有限公司、福建省海峡信息技术有限公司、山东泽鹿安全技术有限公司、内蒙古洞明科技有限公司、重庆都会信息科技有限公司、快页信息技术有限公司、浙江木链物联网科技有限公司、中国烟草总公司湖北省公司、天津偕行科技有限公司、广州易东信息安全技术有限公司、博智安全科技股份有限公司、北京威努特技术有限公司、百度在线网络技术有限公司、苏州棱镜七彩信息科技有限公司、北京水木羽林科技有限公司、中国通信服务重庆公司、北京未来智安科技有限公司、宁波和利时信息安全研究院、北京惠而特科技有限公司及其他个人白帽子向 CNVD 提交了 7905 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）、上海交大和奇安信网神（补天平台）向 CNVD 共享的白帽子报送的 4794 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）	3606	3606
上海交大	772	772
奇安信网神（补天平台）	416	416
北京神州绿盟科技有	310	9

限公司		
哈尔滨安天科技集团股份有限公司	239	0
北京数字观星科技有限公司	218	0
新华三技术有限公司	140	0
恒安嘉新（北京）科技股份公司	122	0
北京启明星辰信息安全技术有限公司	119	3
浙江大华技术股份有限公司	118	118
深信服科技股份有限公司	92	0
天津市国瑞数码安全系统股份有限公司	59	0
华为技术有限公司	50	0
北京天融信网络安全技术有限公司	26	26
西安四叶草信息技术有限公司	16	16
杭州安恒信息技术股份有限公司	10	10
北京长亭科技有限公司	7	7
南京联成科技发展股份有限公司	3	3
深圳市腾讯计算机系统有限公司（玄武实验室）	1	1
沈阳东软系统集成工程有限公司	1	1
贵州多彩宝互联网服务有限公司	351	351
杭州迪普科技股份有	215	200

限公司		
北京华顺信安科技有限公司	182	0
山东云天安全技术有限公司	141	141
北京信联科汇科技有限公司	108	108
杭州海康威视数字技术股份有限公司	98	98
北京山石网科信息技术有限公司	63	63
河南信安世纪科技有限公司	59	59
广东蓝爵网络安全技术股份有限公司	57	57
南京树安信息技术有限公司	49	49
安徽长泰科技有限公司	46	46
长春嘉诚信息技术股份有限公司	43	43
中国电信股份有限公司网络安全产品运营中心	29	29
京东云安全	22	22
联想集团	20	0
北京远禾科技有限公司	20	20
北京云科安信科技有限公司（Seraph 安全实验室）	19	19
河南灵创电子科技有限公司	19	19
北京安帝科技有限公司	18	18

山东新潮信息技术有限公司	15	15
上海纽盾科技股份有限公司	13	13
内蒙古云科数据服务股份有限公司	11	11
福建省海峡信息技术有限公司	11	11
山东泽鹿安全技术有限公司	11	11
内蒙古洞明科技有限公司	7	7
重庆都会信息科技有限公司	7	7
快页信息技术有限公司	6	6
浙江木链物联网科技有限公司	5	5
中国烟草总公司湖北省公司	4	4
天津偕行科技有限公司	4	4
广州易东信息安全技术有限公司	3	3
亚信科技（成都）有限公司	3	0
博智安全科技股份有限公司	2	2
北京威努特技术有限公司	2	2
百度在线网络技术有限公司	2	2
苏州棱镜七彩信息科技有限公司	2	2
北京水木羽林科技有	2	2

限公司		
中国通信服务重庆公司	1	1
北京未来智安科技有限公司	1	1
宁波和利时信息安全研究院	1	1
北京惠而特科技有限公司	1	1
CNCERT 北京分中心	14	14
CNCERT 宁夏分中心	4	4
CNCERT 内蒙古分中心	2	2
CNCERT 河北分中心	1	1
个人	1443	1443
报送总计	9462	7905

本周漏洞按类型和厂商统计

本周，CNVD 收录了 643 个漏洞。WEB 应用 240 个，应用程序 238 个，网络设备（交换机、路由器等网络端设备）111 个，智能设备（物联网终端设备）27 个，操作系统 14 个，安全产品 9 个，数据库 4 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	240
应用程序	238
网络设备（交换机、路由器等网络端设备）	111
智能设备（物联网终端设备）	27
操作系统	14
安全产品	9
数据库	4

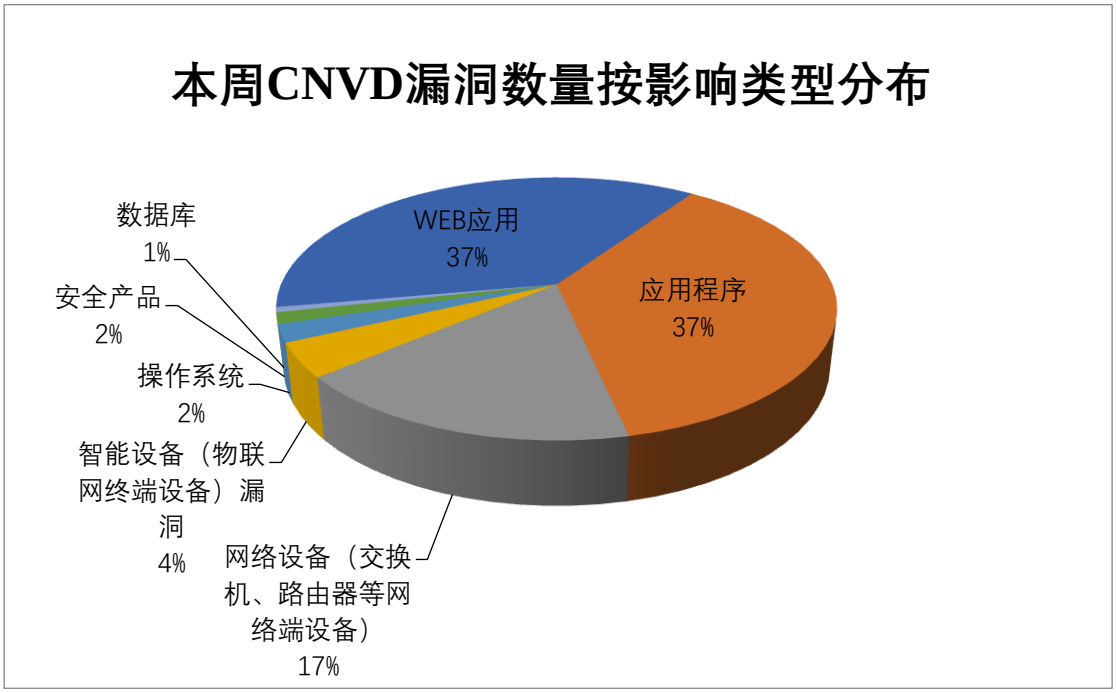

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 XnSoft、哈尔滨伟成科技有限公司、新华三技术有限公司等多家厂商的产品，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	XnSoft	28	4%
2	哈尔滨伟成科技有限公司	24	4%
3	新华三技术有限公司	24	4%
4	智睿软件	20	3%
5	mozilla	17	3%
6	Adobe	16	2%
7	Google	15	2%
8	淄博闪灵网络科技有限公司	14	2%
9	Microsoft	13	2%
10	其他	472	74%

本周行业漏洞收录情况

本周，CNVD 收录了 72 个电信行业漏洞，35 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，“Xiaomi AX3600 命令注入漏洞、Xiaomi AX3600 缓冲区溢出漏洞”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/

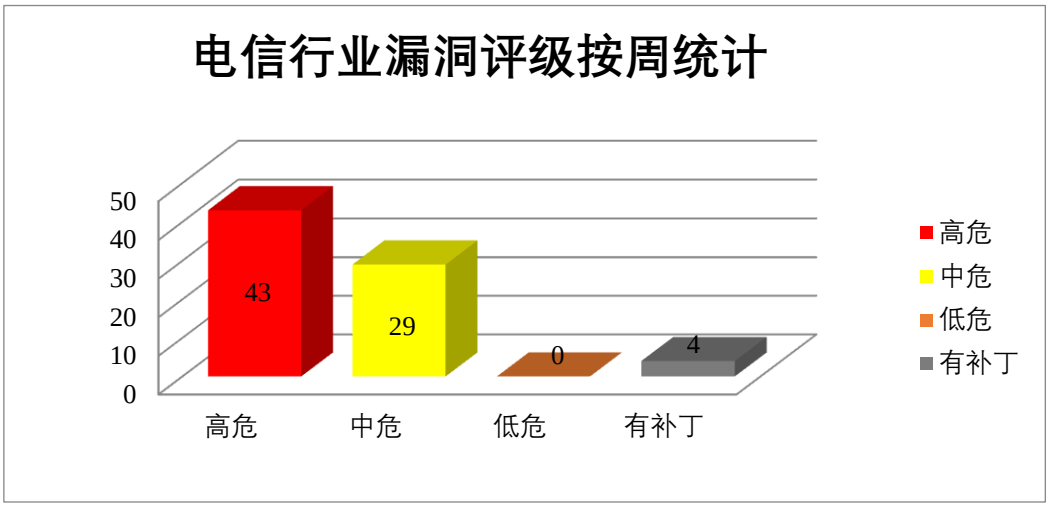

图 3 电信行业漏洞统计

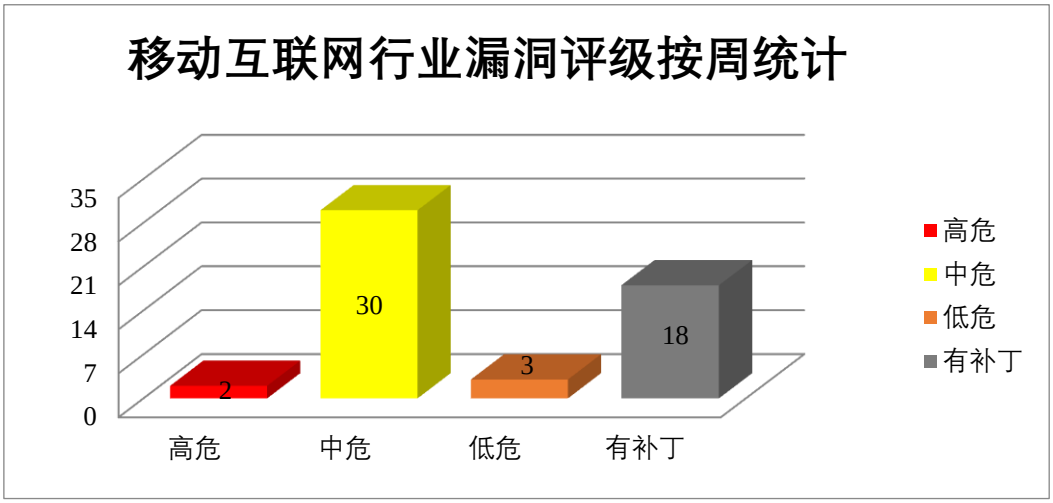

图 4 移动互联网行业漏洞统计

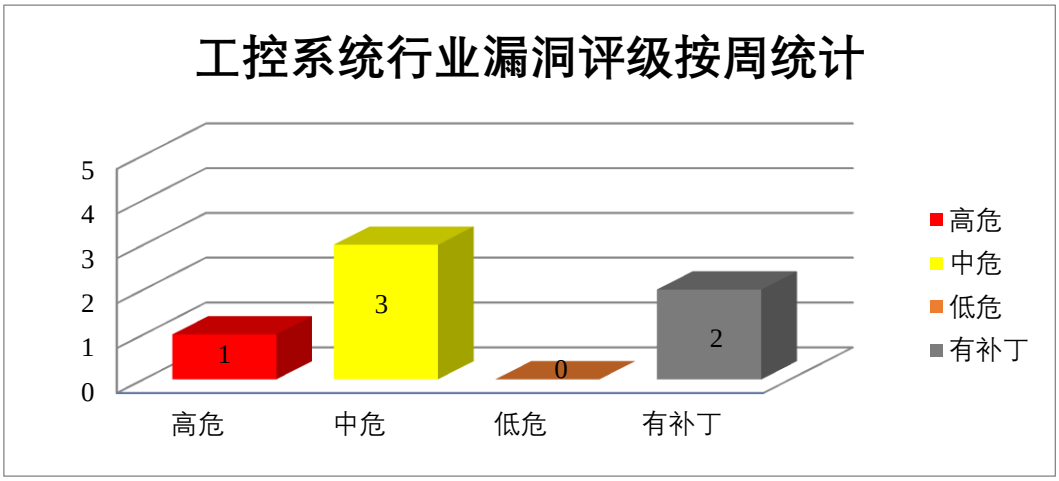

图 5 工控系统行业漏洞统计

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 Exchange Server 是美国微软（Microsoft）公司的一套电子邮件服务程序。它提供邮件存取、储存。转发，语音邮件，邮件过滤筛选等功能。Microsoft Windows 和 Microsoft Windows Server 都是美国微软（Microsoft）公司的产品。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。本周，上述产品被披露存在多个漏洞，攻击者可利用该漏洞提升权限，执行任意代码。

CNVD 收录的相关漏洞包括：Microsoft Exchange Server 远程代码执行漏洞（CNVD-2021-90307）、Microsoft Windows/Windows Server 权限提升漏洞（CNVD-2021-90797、CNVD-2021-90800、CNVD-2021-90799、CNVD-2021-90798、CNVD-2021-90803、CNVD-2021-90802、CNVD-2021-90801）。其中，“Microsoft Windows/Windows Server 权限提升漏洞（CNVD-2021-90800、CNVD-2021-90799、CNVD-2021-90801）”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-2021-90307
https://www.cnvd.org.cn/flaw/show/CNVD-2021-90797
https://www.cnvd.org.cn/flaw/show/CNVD-2021-90800
https://www.cnvd.org.cn/flaw/show/CNVD-2021-90799
https://www.cnvd.org.cn/flaw/show/CNVD-2021-90798
https://www.cnvd.org.cn/flaw/show/CNVD-2021-90803
https://www.cnvd.org.cn/flaw/show/CNVD-2021-90802
https://www.cnvd.org.cn/flaw/show/CNVD-2021-90801

2、 Advantech 产品安全漏洞

Advantech R-SeeNet 是中国台湾研华（Advantech）公司的一个工业监控软件。该软件基于 snmp 协议进行监控平台，并且适用于 Linux。Windows 平台。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞在数据库中执行任意 SQL 查询，升级系统上的权限。

CNVD 收录的相关漏洞包括：Advantech R-SeeNet SQL 注入漏洞（CNVD-2021-90861、CNVD-2021-90869、CNVD-2021-90860、CNVD-2021-90864、CNVD-2021-90863、CNVD-2021-90862、CNVD-2021-90868）、Advantech R-SeeNet 权限提升漏洞。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-2021-90861
https://www.cnvd.org.cn/flaw/show/CNVD-2021-90860

https://www.cnvd.org.cn/flaw/show/CNVD-2021-90864

https://www.cnvd.org.cn/flaw/show/CNVD-2021-90863

https://www.cnvd.org.cn/flaw/show/CNVD-2021-90862

https://www.cnvd.org.cn/flaw/show/CNVD-2021-90867

https://www.cnvd.org.cn/flaw/show/CNVD-2021-90869

https://www.cnvd.org.cn/flaw/show/CNVD-2021-90868

3、 Adobe 产品安全漏洞

Adobe After Effects（简称“AE”）是 Adobe 公司推出的一款图形视频处理软件，适用于从事设计和视频特技的机构，包括电视台、动画制作公司，个人后期制作工作室以及多媒体工作室。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：Adobe After Effects 内存缓冲区越界访问漏洞（CNVD-2021-89928、CNVD-2021-89937、CNVD-2021-89929、CNVD-2021-89930、CNVD-2021-89931、CNVD-2021-89932、CNVD-2021-89935、CNVD-2021-89934）。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-2021-89928

https://www.cnvd.org.cn/flaw/show/CNVD-2021-89929

https://www.cnvd.org.cn/flaw/show/CNVD-2021-89930

https://www.cnvd.org.cn/flaw/show/CNVD-2021-89931

https://www.cnvd.org.cn/flaw/show/CNVD-2021-89932

https://www.cnvd.org.cn/flaw/show/CNVD-2021-89935

https://www.cnvd.org.cn/flaw/show/CNVD-2021-89934

https://www.cnvd.org.cn/flaw/show/CNVD-2021-89937

4、 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提升权限，执行任意代码等。

CNVD 收录的相关漏洞包括：Mozilla Firefox 拒绝服务漏洞（CNVD-2021-89693）、Mozilla Firefox 缓冲区溢出漏洞（CNVD-2021-89692、CNVD-2021-90097、CNVD-2021-90096、CNVD-2021-90100、CNVD-2021-90103）、Mozilla Firefox 权限许可和访问控制问题漏洞（CNVD-2021-90104、CNVD-2021-90106）。其中，“Mozilla Firefox 拒绝服务漏洞（CNVD-2021-89693）、Mozilla Firefox 权限许可和访问控制问题漏洞（CNVD-2021-90104）”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-2021-89693

https://www.cnvd.org.cn/flaw/show/CNVD-2021-89692

https://www.cnvd.org.cn/flaw/show/CNVD-2021-90097

https://www.cnvd.org.cn/flaw/show/CNVD-2021-90096

https://www.cnvd.org.cn/flaw/show/CNVD-2021-90100

https://www.cnvd.org.cn/flaw/show/CNVD-2021-90104

https://www.cnvd.org.cn/flaw/show/CNVD-2021-90103

https://www.cnvd.org.cn/flaw/show/CNVD-2021-90106

5、Amazon AWS SDK 信息泄露漏洞

Amazon AWS SDK for Android 是美国亚马逊（Amazon）公司的一款基于 Android 平台的用于 Amazon Web Services（AWS）的软件开发工具包。本周，Amazon AWS SDK 1.7.22 及之前版本被披露存在信息泄露漏洞。攻击者可利用该漏洞通过读取程序中以明文形式存储的凭据访问 AWS S3 开发人员文件导致信息泄露。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-2021-91630

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-2021-89684	MedData Hbys SQL 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://gist.github.com/Blackh4n/9d8feaf1cfb68f66de17361e85f616d4
CNVD-2021-89682	Apache ShenYu 授权问题漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://lists.apache.org/thread/o15j25qwtpcw62k48xw1tnv48skh3zgb
CNVD-2021-89936	Adobe After Effects 内存缓冲区越界访问漏洞（CNVD-2021-89936）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://helpx.adobe.com/security/products/after_effects/apsb21-79.html
CNVD-2021-89941	Moxa MXview 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.moxa.com/en/support/product-support/software-and-documentation/search?psid=53389
CNVD-2021-90092	Wireshark 空指针解引用漏洞（CNVD-2021-90092）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.wireshark.org/security/wnpa-sec-2021-15.html

CNVD-2021-90866	Advantech R-SeeNet 不正确默认权限漏洞（CNVD-2021-90866）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://talosintelligence.com/vulnerability_reports/TALOS-2021-1360
CNVD-2021-90919	Nagios XI 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.nagios.com/downloads/nagios-xi/change-log/
CNVD-2021-91275	Synapse 路径遍历漏洞	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/matrix-org/synapse/security/advisories/GHSA-3hfw-x7gx-437c
CNVD-2021-91282	Vim 缓冲区溢出漏洞（CNVD-2021-91282）	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/vim/vim
CNVD-2021-91284	Google Chrome contacts picker 安全绕过漏洞	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://chromereleases.googleblog.com/2021/11/stable-channel-update-for-desktop.html

小结：本周，Microsoft 产品被披露存在多个漏洞，攻击者可利用该漏洞提升权限，执行任意代码。此外，Advantech，Adobe，Mozilla 等多款产品被披露存在多个漏洞，攻击者可利用漏洞在数据库中执行任意 SQL 查询，提升权限，执行任意代码等。另外，Amazon AWS SDK 1.7.22 及之前版本被披露存在信息泄露漏洞。攻击者可利用该漏洞通过读取程序中以明文形式存储的凭据访问 AWS S3 开发人员文件导致信息泄露。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、Hitachi Vantara Pentaho 访问控制错误漏洞

验证描述

Hitachi Vantara Pentaho 是日本 Hitachi 公司的一款用于大数据环境中对数据进行存储和管理的服务。

Hitachi Vantara Pentaho 存在访问控制错误漏洞，攻击者可利用该漏洞列出 Jackrabbit 存储库中存在的所有应用程序用户名。

验证信息

POC 链接：https://packetstormsecurity.com/files/164787/Pentaho-Business-Analytics-P

entaho-Business-Server-9.1-User-Enumeration.html

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2021-90770

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. Oracle VirtualBox 存在安全漏洞

近期，专家披露了甲骨文 VirtualBox 中的漏洞（编号为 CVE-2021-2442），该漏洞可能会被用于破坏虚拟机管理程序并触发拒绝服务（DoS）条件。

参考链接：https://www.freebuf.com/news/305918.html

2. 思科 Talos 发现一个高危提权漏洞，所有 Windows 版本均受影响

计算机安全组织 Cisco Talos 发现了一个新的提权漏洞，该漏洞存在 Windows 安装程序中，包括 Windows 11 和 Windows Server 2022 在内的所有 Windows 版本均受影响。

参考链接：https://www.cnbeta.com/articles/tech/1207121.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