国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2022 年 10 月 10 日-2022 年 10 月 16 日 **2022 年第 41 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 447 个，其中高危漏洞 172 个、中危漏洞 217 个、低危漏洞 58 个。漏洞平均分值为 6.29。本周收录的漏洞中，涉及 0day 漏洞 213 个（占 48%），其中互联网上出现“Trendnet IP-110wn proname 参数跨站脚本漏洞、NETGEAR WNAP320 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漏洞总数 14785 个，与上周（22950 个）环比减少 36%。

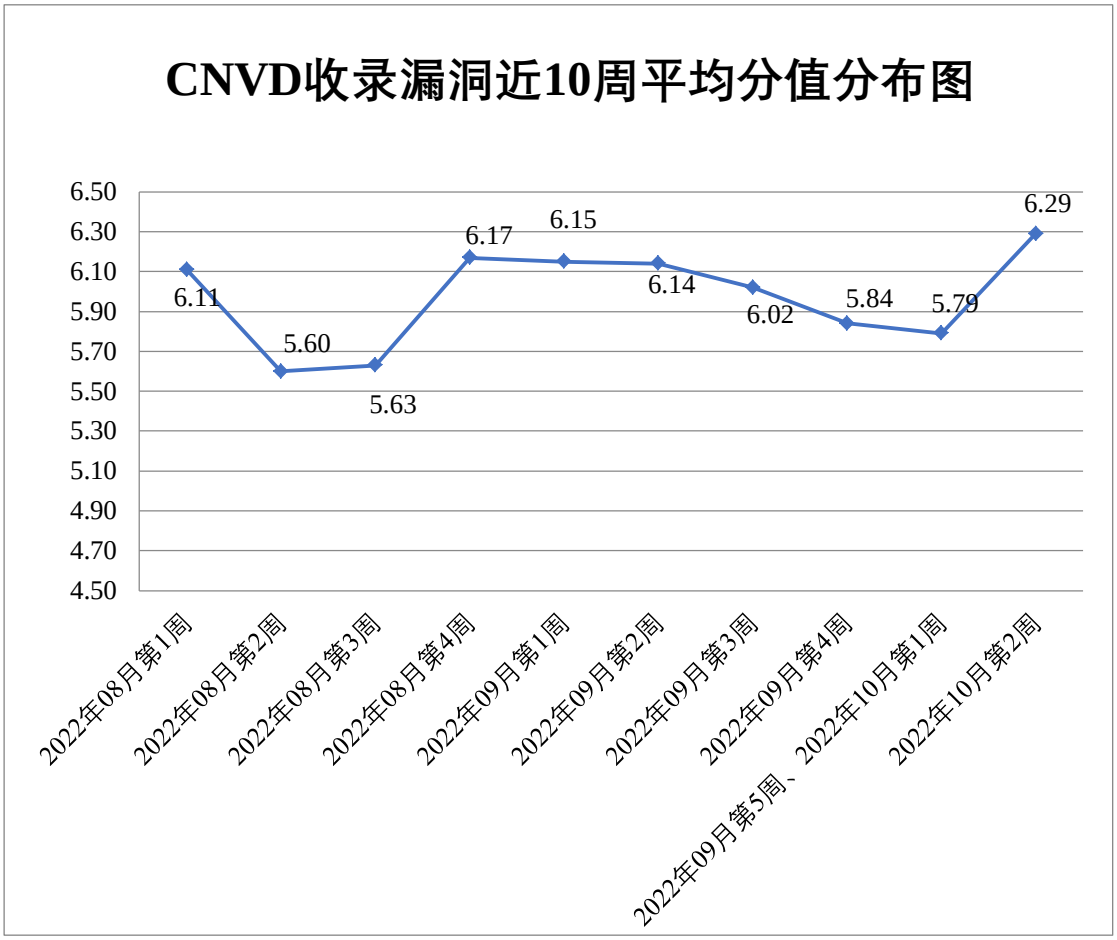

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 22 起，向基础电信企业通报漏洞事件 16 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 466 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 197 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 79 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、珠海金山办公软件有限公司、重庆中誉霖齐实业（集团）有限公司、重庆森鑫炬科技有限公司 、重庆森鑫炬科技有限公司、重庆巨泰物联网集团有限公司、中科数字通（北京）科技有限公司、浙江兰德纵横网络技术股份有限公司、浙江海看科技集团有限公司、长沙雷电云网络科技有限公司、友讯电子设备（上海）有限公司、优酷信息技术（北京）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、武汉微问网络科技有限公司、武汉华中数控股份有限公司、武汉地大信息工程股份有限公司、天津恒企财务信息咨询有限公司、天地伟业技术有限公司、四平市九州易通科技有限公司、四川迅睿云软件开发有限公司、四川天邑康和通信股份有限公司、四川袋临天下新材料有限公司、施耐德电气（中国）有限公司、深圳维盟科技股份有限公司、深圳市子辰视讯科技有限公司、深圳市兴海物联科技有限公司、深圳市唯德科创信息有限公司、深圳市网是科技有限公司、深圳市思迅软件股份有限公司、深圳市仁清卓越科技有限公司、深圳市吉祥腾达科技有限公司、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、深圳市瀚兰区块链地产有限公司、深圳市丛文科技有限公司、深圳市必联电子有限公司、深圳昆仑通态科技有限责任公司、深圳警翼智能科技股份有限公司、上海纵之格科技有限公司、上海卓卓网络科技有限公司、上海源天软件有限公司、上海上业信息科技股份有限公司、上海森栩医学科技有限公司、上海脉信网络科技有限公司、上海迈微软件科技有限公司、上海会畅通讯股份有限公司、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、上海超维健康管理有限公司、上海百酷信息科技有限公司、熵基科技股份有限公司、山西企凝信息科技有限公司、山东中创软件商用中间件股份有限公司、山东山大华天软件有限公司、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、赛云九洲科技股份有限公司、任子行网络技术股份有限公司、确信信息股份有限公司、青果软件集团有限公司、秦皇岛市创想信息网络有限公司、普联技术有限公司、南通润邦网络科技有限公司、南京来势科技公司、美图公司、迈普通信技术股份有限公司、廊坊市极致网络科技有限公司、江

苏省广电有线信息网络股份有限公司、江苏赛达电子科技有限公司、吉翁电子（深圳）有限公司、汇链科技有限公司、湖南翱云网络科技有限公司、恒锋信息科技股份有限公司、河南立程起才汽车租赁有限公司、杭州雄伟科技开发股份有限公司、杭州可道云网络有限公司、杭州海康威视系统技术有限公司、杭州博采网络科技股份有限公司、海南有趣科技有限公司、贵州觅新科技有限公司、广州同鑫科技有限公司、广州市开利网络科技有限公司、广州市保伦电子有限公司、广州市奥威亚电子科技有限公司、广州点步信息科技有限公司、广东盈世计算机科技有限公司、福建淘客互动网络科技有限公司、福建博思软件股份有限公司、伏能士智能设备(上海)有限公司、飞思达技术（北京）有限公司、鼎捷软件股份有限公司、大连卓云科技有限公司、创辉科技有限公司、成都友加畅捷科技有限公司、成都依能科技股份有限公司、成都市智蜂网科技有限责任公司、成都华栖云科技有限公司、成都海信达科技有限公司、成都飞鱼星科技股份有限公司、畅捷通信息技术股份有限公司、北京中广上洋科技股份有限公司、北京中创视讯科技有限公司、北京星网锐捷网络技术有限公司、北京网动网络科技股份有限公司、北京万户网络技术有限公司、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、北京如易行科技有限公司、北京奇虎科技有限公司、北京派网软件有限公司、北京龙软科技股份有限公司、北京乐嗨科技有限公司、北京凯特伟业科技有限公司、北京金和网络股份有限公司、北京车之家信息技术有限公司、北京百卓网络技术有限公司、北京百度网讯科技有限公司、包头市助友科技有限公司、傲拓科技股份有限公司、阿里巴巴集团安全应急响应中心和 SEMCMS。

本周，CNVD 发布了《Microsoft 发布 2022 年 10 月安全更新》。详情参见 CNVD 网站公告内容。

https://www.cnvd.org.cn/webinfo/show/8176

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，新华三技术有限公司、深信服科技股份有限公司、安天科技集团股份有限公司、阿里云计算有限公司、南京众智维信息科技有限公司等单位报送公开收集的漏洞数量较多。北京华顺信安信息技术有限公司、快页信息技术有限公司、安徽锋刃信息科技有限公司、山东云天安全技术有限公司、河南信安世纪科技有限公司、北京山石网科信息技术有限公司、重庆都会信息科技有限公司、河南东方云盾信息技术有限公司、奇安星城网络安全运营服务（长沙）有限公司、江西和尔惠信息技术有限公司、北京云科安信科技有限公司（Seraph 安全实验室）、北京六方云信息技术有限公司、北京安帝科技有限公司、成方金融科技有限公司上海分公司、上海纽盾科技股份有限公司、山石网科通信技术股份有限公司、湖北珞格科技发展有限公司、河南悦海数安科技有限公司、苏州棱镜七彩信息科技有限公司、广东唯顶信息科技股份有限公

司、浙江木链物联网科技有限公司、中国电信股份有限公司网络安全产品运营中心、联通数字科技有限公司、山东新潮信息技术有限公司、长春嘉诚信息技术股份有限公司、贵州泰若数字科技有限公司、杭州默安科技有限公司、北京微步在线科技有限公司、广州安亿信软件科技有限公司、南京禾盾信息科技有限公司、博智安全科技股份有限公司、中通服创发科技有限责任公司及其他个人白帽子向 CNVD 提交了 14785 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 12957 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）	12039	12039
新华三技术有限公司	542	0
上海交大	522	522
奇安信网神（补天平台）	396	396
深信服科技股份有限公司	304	0
安天科技集团股份有限公司	224	0
阿里云计算有限公司	179	0
南京众智维信息科技有限公司	175	175
远江盛邦（北京）网络安全科技股份有限公司	155	155
恒安嘉新（北京）科技股份公司	105	0
北京数字观星科技有限公司	95	0
西安四叶草信息技术有限公司	76	76
杭州安恒信息技术股份有限公司	68	64
卫士通信息产业股份有限公司	13	13
内蒙古云科数据服务	12	12

股份有限公司		
北京知道创宇信息技术有限公司	15	0
北京天融信网络安全技术有限公司	7	7
北京智游网安科技有限公司	3	3
北京信联科汇科技有限公司	1	1
北京启明星辰信息安全技术有限公司	1	1
北京华顺信安信息技术有限公司	199	5
快页信息技术有限公司	47	47
安徽锋刃信息科技有限公司	23	23
杭州迪普科技股份有限公司	19	0
山东云天安全技术有限公司	16	16
河南信安世纪科技有限公司	14	14
北京山石网科信息技术有限公司	13	13
重庆都会信息科技有限公司	12	12
河南东方云盾信息技术有限公司	10	10
奇安星城网络安全运营服务（长沙）有限公司	9	9
江西和尔惠信息技术有限公司	9	9
北京云科安信科技有	9	9

限公司（Seraph 安全实验室）		
北京六方云信息技术有限公司	7	7
北京安帝科技有限公司	6	6
成方金融科技有限公司上海分公司	4	4
上海纽盾科技股份有限公司	4	4
山石网科通信技术股份有限公司	4	4
湖北珞格科技发展有限公司	3	3
河南悦海数安科技有限公司	3	3
苏州棱镜七彩信息科技有限公司	3	3
广东唯顶信息科技股份有限公司	3	3
浙江木链物联网科技有限公司	3	3
中国电信股份有限公司网络安全产品运营中心	2	2
联通数字科技有限公司	2	2
山东新潮信息技术有限公司	2	2
长春嘉诚信息技术股份有限公司	2	2
贵州泰若数字科技有限公司	2	2
杭州默安科技有限公司	2	2

北京微步在线科技有限公司	2	2
亚信科技（成都）有限公司	1	0
广州安亿信软件科技有限公司	1	1
南京禾盾信息科技有限公司	1	1
博智安全科技股份有限公司	1	1
中通服创发科技有限责任公司	1	1
CNCERT 内蒙古分中心	6	6
CNCERT 四川分中心	2	2
CNCERT 贵州分中心	2	2
个人	1086	1086
报送总计	16467	14785

本周漏洞按类型和厂商统计

本周，CNVD 收录了 447 个漏洞。WEB 应用 217 个，应用程序 122 个，网络设备（交换机、路由器等网络端设备）58 个，操作系统 33 个，安全产品 10 个，智能设备（物联网终端设备）7 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	217
应用程序	122
网络设备（交换机、路由器等网络端设备）	58
操作系统	33
安全产品	10
智能设备（物联网终端设备）	7

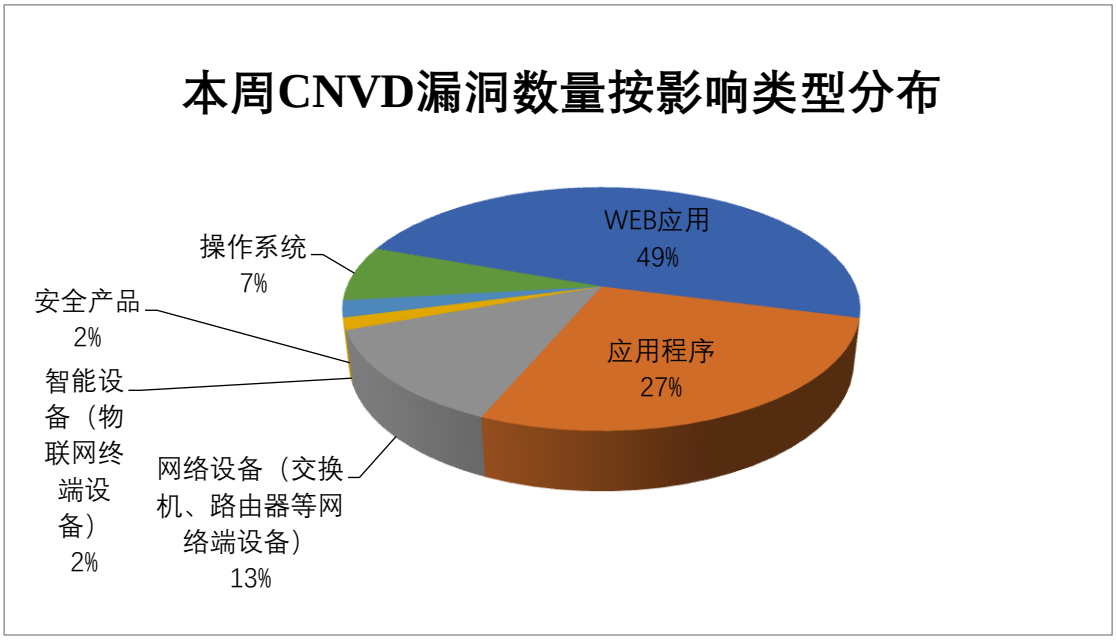

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 WordPress、Vim、Linux 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	WordPress	55	13%
2	Vim	27	6%
3	Linux	18	4%
4	ARRIS	13	3%
5	itsourcecode	12	3%
6	Synology	11	2%
7	Adobe	11	2%
8	Online Banking System	10	2%
9	Microsoft	10	2%
10	其他	280	63%

本周行业漏洞收录情况

本周，CNVD 收录了 43 个电信行业漏洞，20 个移动互联网行业漏洞，7 个工控行业漏洞（如下图所示）。其中，“ASUS RT-AX56U 缓冲区溢出漏洞、TP-LINK AX10 代码注入漏洞”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/

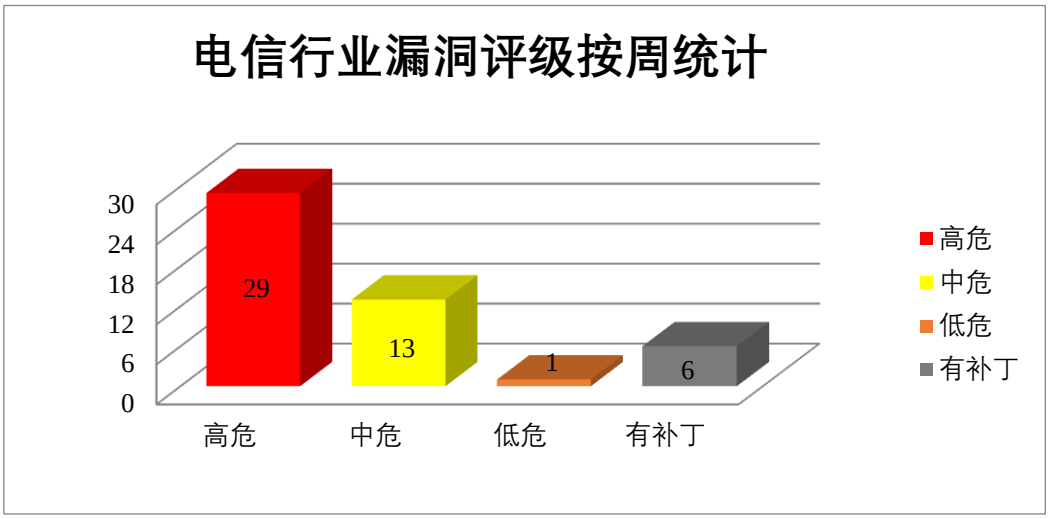

图 3 电信行业漏洞统计

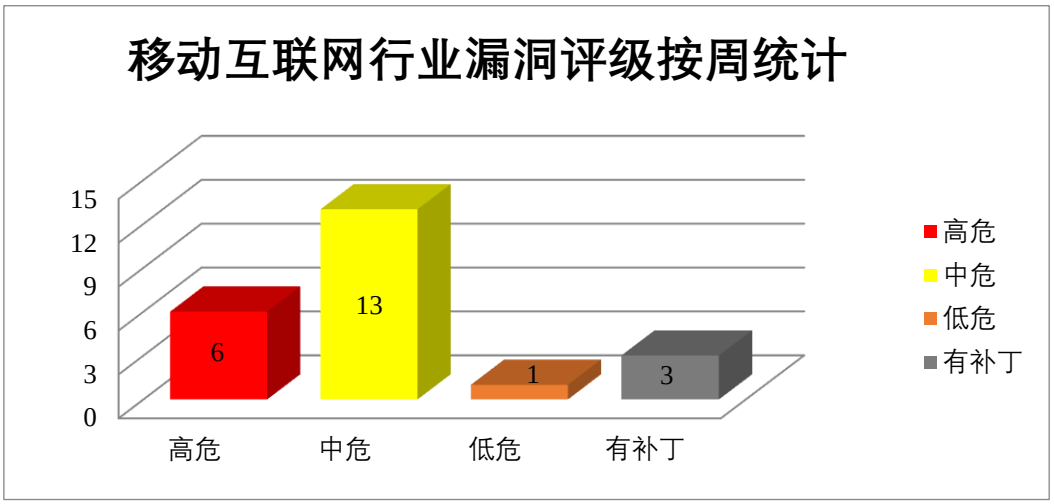

图 4 移动互联网行业漏洞统计

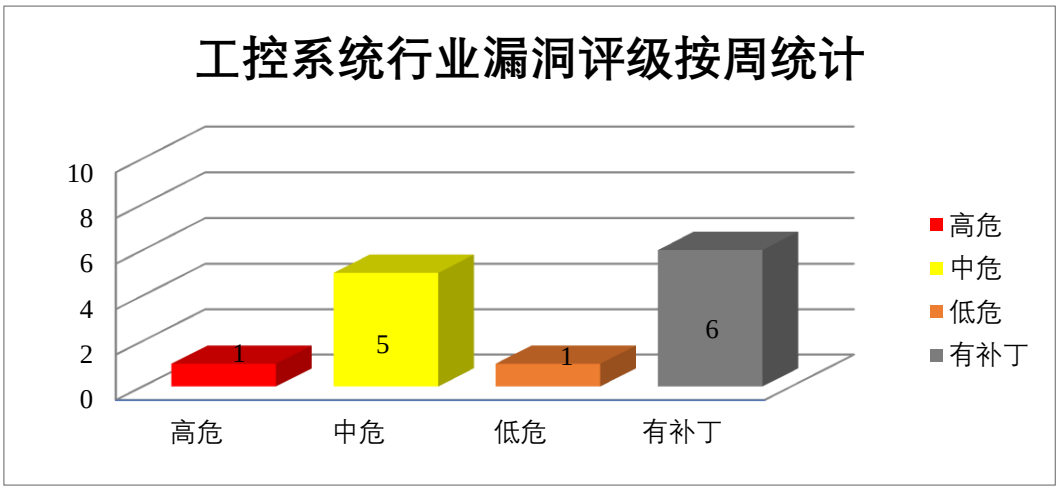

图 5 工控系统行业漏洞统计

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 Exchange Server 是一款微软开发的流行的邮件服务程序。Microsoft Azure Site Recovery(ASR)是 Azure 提供的一种 DRaaS，用于云和混合云架构。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞提交特殊的请求，可通过 PowerShell 以应用程序上下文执行任意代码，可获取敏感信息或者提升权限等。

CNVD 收录的相关漏洞包括：Microsoft Exchange Server 远程代码执行漏洞（CNVD-2022-67838）、Microsoft Exchange Server 权限提升漏洞（CNVD-2022-67837）、Microsoft Azure Site Recovery 远程代码执行漏洞（CNVD-2022-67840）、Microsoft Azure Site Recovery 权限提升漏洞（CNVD-2022-67842、CNVD-2022-67841、CNVD-2022-67845、CNVD-2022-67844、CNVD-2022-67843）。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-2022-67838
https://www.cnvd.org.cn/flaw/show/CNVD-2022-67837
https://www.cnvd.org.cn/flaw/show/CNVD-2022-67842
https://www.cnvd.org.cn/flaw/show/CNVD-2022-67841
https://www.cnvd.org.cn/flaw/show/CNVD-2022-67840
https://www.cnvd.org.cn/flaw/show/CNVD-2022-67845
https://www.cnvd.org.cn/flaw/show/CNVD-2022-67844
https://www.cnvd.org.cn/flaw/show/CNVD-2022-67843

2、 Synology 产品安全漏洞

Synology DiskStation Manager (DSM)是中国台湾群晖科技（Synology）公司的一套用于网络储存服务器（NAS）上的操作系统。该操作系统可管理资料、文件、照片、音乐等信息。Synology WebDAV Server 是一个 HTTP 的扩充服务，可让用户编辑和管理存储在远程服务器上的文件。Synology Media Server 是一个媒体服务器。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞向任意路径写入文件，删除任意文件，执行任意代码等。

CNVD 收录的相关漏洞包括：Synology DiskStation Manager 信息泄露漏洞（CNVD-2022-67834）、Synology DiskStation Manager 注入漏洞（CNVD-2022-67835）、Synology DiskStation Manager 路径遍历漏洞（CNVD-2022-67836、CNVD-2022-67856）、Synology DiskStation Manager 缓冲区溢出漏洞、Synology DiskStation Manager 命令注入漏洞（CNVD-2022-67853）、Synology WebDAV Server 路径遍历漏洞、Synology Media Server 信息泄露漏洞。其中，“Synology DiskStation Manager 缓冲区溢出漏洞、Synology DiskStation Manager 路径遍历漏洞（CNVD-2022-67856）、Synology WebDAV

Server 路径遍历漏洞、Synology Media Server 信息泄露漏洞”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-2022-67834
https://www.cnvd.org.cn/flaw/show/CNVD-2022-67835
https://www.cnvd.org.cn/flaw/show/CNVD-2022-67836
https://www.cnvd.org.cn/flaw/show/CNVD-2022-67847
https://www.cnvd.org.cn/flaw/show/CNVD-2022-67853
https://www.cnvd.org.cn/flaw/show/CNVD-2022-67856
https://www.cnvd.org.cn/flaw/show/CNVD-2022-67857
https://www.cnvd.org.cn/flaw/show/CNVD-2022-67858

3、 Adobe 产品安全漏洞

Adobe Character Animator 是美国奥多比（Adobe）公司的一款动作捕捉和动画制作工具。Adobe Acrobat 是一套 PDF 文件编辑和转换工具。Adobe Reader 是一套 PDF 文档阅读软件。Adobe After Effects 是一套视觉效果和动态图形制作软件。该软件主要用于 2D 和 3D 合成、动画制作和视觉特效制作等。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞在当前用户的上下文中执行任意代码，导致敏感内存泄露，应用程序拒绝服务等。

CNVD 收录的相关漏洞包括：Adobe Character Animator 2021 越界读取漏洞（CNVD-2022-67828、CNVD-2022-67831）、Adobe Character Animator 2021 内存损坏漏洞（CNVD-2022-67832、CNVD-2022-67833）、Adobe Character Animator 2021 内存缓冲区越界访问漏洞（CNVD-2022-67830）、多款 Adobe 产品资源管理错误漏洞（CNVD-2022-67850）、Adobe After Effects 缓冲区溢出漏洞（CNVD-2022-67849、CNVD-2022-67848）。其中，除“Adobe Character Animator 2021 越界读取漏洞（CNVD-2022-67828、CNVD-2022-67831）、Adobe Character Animator 2021 内存缓冲区越界访问漏洞（CNVD-2022-67830）”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-2022-67828
https://www.cnvd.org.cn/flaw/show/CNVD-2022-67832
https://www.cnvd.org.cn/flaw/show/CNVD-2022-67831
https://www.cnvd.org.cn/flaw/show/CNVD-2022-67830
https://www.cnvd.org.cn/flaw/show/CNVD-2022-67833
https://www.cnvd.org.cn/flaw/show/CNVD-2022-67850
https://www.cnvd.org.cn/flaw/show/CNVD-2022-67849

https://www.cnvd.org.cn/flaw/show/CNVD-2022-67848

4、Linux 产品安全漏洞

Linux kernel 是美国 Linux 基金会的开源操作系统 Linux 所使用的内核。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞获得对某些数据的未经授权访问，获得提升的权限并在内核上下文中执行任意代码等。

CNVD 收录的相关漏洞包括：Linux kernel 拒绝服务漏洞、Linux kernel 权限提升漏洞（CNVD-2022-68560、CNVD-2022-68577、CNVD-2022-68594、CNVD-2022-68618）、Linux kernel 缓冲区溢出漏洞（CNVD-2022-68570、CNVD-2022-68616）、Linux kernel 内存泄露漏洞（CNVD-2022-68574）。其中，“Linux kernel 权限提升漏洞（CNVD-2022-68618、CNVD-2022-68560、CNVD-2022-68577）、Linux kernel 缓冲区溢出漏洞（CNVD-2022-68616）”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-2022-68510

https://www.cnvd.org.cn/flaw/show/CNVD-2022-68560

https://www.cnvd.org.cn/flaw/show/CNVD-2022-68570

https://www.cnvd.org.cn/flaw/show/CNVD-2022-68574

https://www.cnvd.org.cn/flaw/show/CNVD-2022-68577

https://www.cnvd.org.cn/flaw/show/CNVD-2022-68594

https://www.cnvd.org.cn/flaw/show/CNVD-2022-68616

https://www.cnvd.org.cn/flaw/show/CNVD-2022-68618

5、NETGEAR R7000 缓冲区溢出漏洞（CNVD-2022-69163）

NETGEAR R7000 是美国网件（NETGEAR）公司的一款无线路由器。本周，NETGEAR R7000 被披露存在缓冲区溢出漏洞。攻击者可以利用该漏洞执行非授权指令，可以取得系统特权，进而进行各种非法操作。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-2022-69163

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-2022-67839	Microsoft Visual Studio 远程代码执行漏洞（CNVD-2022-67839）	高	目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载：https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-35825

CNVD-2022-67846	Microsoft Exchange Server 特权提升漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24477
CNVD-2022-68078	Vim 资源管理错误漏洞（CNVD-2022-68078）	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/commit/1c3dd8ddcba63c1af5112e567215b3cec2de11d0
CNVD-2022-68080	Zyxel CloudCNM SecuManager axiros 默认账户漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://www.zyxel.com/support/vulnerabilities-of-CloudCNM-SecuManager.shtml
CNVD-2022-68084	Vim 资源管理错误漏洞（CNVD-2022-68084）	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/commit/ccfde4d028e891a41e3548323c3d47b06fb0b83e
CNVD-2022-68082	Zyxel CloudCNM SecuManager 信任管理问题漏洞（CNVD-2022-68082）	高	用户可参考如下厂商提供的安全补丁以修复该漏洞： https://www.zyxel.com/support/vulnerabilities-of-CloudCNM-SecuManager.shtml
CNVD-2022-68081	Zyxel CloudCNM SecuManager /opt/axess/etc/default/axess 硬编码漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://www.zyxel.com/support/vulnerabilities-of-CloudCNM-SecuManager.shtml
CNVD-2022-68099	Vim 缓冲区溢出漏洞（CNVD-2022-68099）	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/commit/dbdd16b62560413abcc3c8e893cc3010ccf31666
CNVD-2022-68104	Vim 资源管理错误漏洞（CNVD-2022-68104）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/vim/vim/commit/1889f499a4f248cd84e0e0bf6d0d820016774494
CNVD-2022-68273	Metersphere 任意文件上传漏洞	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/metersphere/metersphere/releases/tag/v1.20.15-lts

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交特殊的请

求，可通过 PowerShell 以应用程序上下文执行任意代码，可获取敏感信息或者提升权限等。此外，Synology、Adobe、Linux 等多款产品被披露存在多个漏洞，攻击者可利用漏洞在当前用户的上下文中执行任意代码，导致敏感内存泄露，应用程序拒绝服务，向任意路径写入文件，删除任意文件，提升权限等。另外，NETGEAR R7000 被披露存在缓冲区溢出漏洞。攻击者可利用漏洞执行非授权指令，可以取得系统特权，进而进行各种非法操作。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、NETGEAR WNAP320 访问控制错误漏洞

验证描述

NETGEAR WNAP320 是美国网件（NETGEAR）公司的一款无线接入点（AP）。

NETGEAR WNAP320 v2.0.3 版本存在访问控制错误漏洞，该漏洞源于/recreate.php 存在错误的访问控制，攻击者可利用该漏洞获取用户的 cookie。

验证信息

POC 链接：https://github.com/jayus0821/uai-poc/blob/main/Netgear/WNAP320/unauth.md

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2022-68507

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. Fortinet 身份验证绕过漏洞的 POC 已经发布

最近披露的影响 Fortinet FortiOS、FortiProxy 和 FortiSwitchManager 的安全漏洞已提供概念验证(PoC)漏洞利用代码，因此用户需要尽快采取措施加以防范。

参考链接：https://thehackernews.com/2022/10/poc-exploit-released-for-critical.html

2. 最新发现的西门子工业网络软件漏洞已影响多款产品

西门子 Simatic 可编程逻辑控制器（PLC）的一个漏洞可被利用，以检索硬编码的全球私人加密密钥并夺取设备的控制权。

参考链接：https://www.sohu.com/a/592604688_257305

关于 CNVD

国家信息安全漏洞共享平台（China National Vulnerability Database，简称 CNVD）是由 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国家网络安全漏洞库，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，是我国计算机网络应急处理体系中的牵头单位。

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