国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2022 年 07 月 11 日-2022 年 07 月 17 日 **2022 年第 28 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 474 个，其中高危漏洞 208 个、中危漏洞 225 个、低危漏洞 41 个。漏洞平均分值为 6.21。本周收录的漏洞中，涉及 0day 漏洞 317 个（占 67%），其中互联网上出现“H3C Magic R100 缓冲区溢出漏洞（CNVD-2022-50705）、TOTOLINK N600R 缓冲区溢出漏洞”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 6909 个，与上周（7858 个）环比减少 12%。

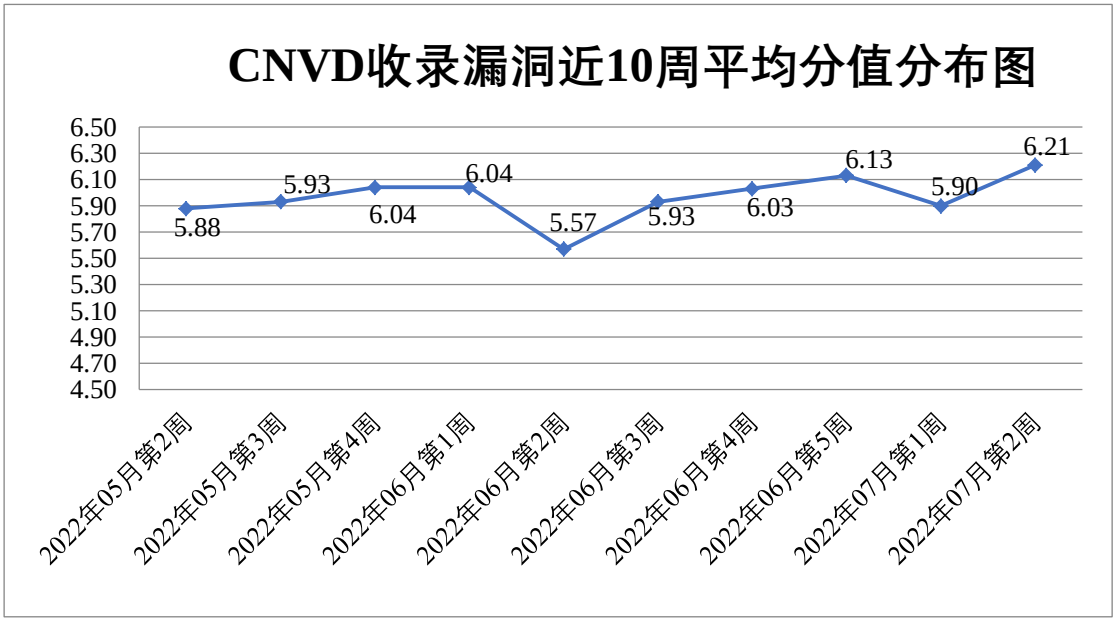

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 22 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 507 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 124 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 86 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、珠海新华通软件股份有限公司、珠海派诺科技股份有限公司、浙江大华技术股份有限公司、友讯电子设备（上海）有限公司、友德信息技术股份有限公司、用友网络科技股份有限公司、兄弟（中国）商业有限公司、西银澎程科技有限公司、武汉宏图博创网络科技有限公司、卫宁健康科技集团股份有限公司、松下电器（中国）有限公司、四平市九州易通科技有限公司、四川迅睿云软件开发有限公司、四川省宏业建设软件有限责任公司、思科系统（中国）网络技术有限公司、深圳市亿图软件有限公司、深圳市万网博通科技有限公司、深圳市领空技术有限公司、深圳市聚网捷科技有限公司、深圳市吉祥腾达科技有限公司、上海卓卓网络科技有限公司、上海新时达机器人有限公司、上海汉得信息技术股份有限公司、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、上海步科自动化股份有限公司、上海贝锐信息科技股份有限公司、熵基科技股份有限公司、山东金钟科技集团股份有限公司、厦门网中网软件有限公司、厦门四信通信科技有限公司、森净科技股份有限公司、麒麟软件有限公司、普联技术有限公司、南通润邦网络科技有限公司、南京海比信息技术有限公司、南京埃斯顿自动化股份有限公司、南昌腾速科技有限公司、理光（中国）投资有限公司、廊坊市极致网络科技有限公司、金蝶软件（中国）有限公司、江西金磊科技发展有限公司、江苏三恒科技股份有限公司、佳能（中国）有限公司、惠普贸易（上海）有限公司、湖南建研信息技术股份有限公司、恒锋信息科技股份有限公司、河南摩尔水溶肥料有限公司、好嗨油能源科技（河南）有限公司、杭州海康威视数字技术股份有限公司、杭州海康存储科技有限公司、杭州迪普科技股份有限公司、汉王科技股份有限公司、广州图创计算机软件开发有限公司、广州恒企教育科技有限公司、广州好象科技有限公司、广州超远机电科技有限公司、福州银达云创信息科技有限公司、福州网钛软件科技有限公司、东营金石软件有限公司、东莞市智跃软件科技有限公司、创维集团有限公司、畅捷通信息技术股份有限公司、常州瑞信电子科技有限公司、北京中创视讯科技有限公司、北京智慧远景科技产业有限公司、北京逸群信息有限公司、北京星网锐捷网络技术有限公司、北京万方数据股份有限公司、北京统御至诚科技有限公司、北京通达信科科技有限公司、北京圣博润高新技术股份有限公司、北京力控元通科技有限公司、北京九思协同软件有限公司、北京金和网络股份有限公司、北京华夏创新科技有限公司、北京国炬信息技术有限公司、北京国栋科技有限公司、北京点为信息科技有限公司、北京超图软件股份有限公司、北京宝兰德软件股份有限公司、北京百卓网络技术有限公司、暴风集团股份有限公司、百驿物联股份有限公司、奥祥网络科技、阿

里巴巴集团安全应急响应中心、三菱电机株式会社、华夏 ERP、WAVLINK、ZZCMS、YIXUNCMS、WAVLINK、The Apache Software Foundation、SEMCMS、SEACMS、OwnCloud、NETGEAR、MuYuCMS 和 ACME Laboratories。

本周，CNVD 发布了《Microsoft 发布 2022 年 6 月安全更新》。详情参见 CNVD 网站公告内容。

https://www.cnvd.org.cn/webinfo/show/7891

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、北京神州绿盟科技有限公司、北京数字观星科技有限公司、安天科技集团股份有限公司等单位报送公开收集的漏洞数量较多。北京华顺信安科技有限公司、西门子（中国）有限公司、山石网科通信技术股份有限公司、河南东方云盾信息技术有限公司、上海嘉韦思信息技术有限公司、星云博创科技有限公司、广州易东信息安全技术有限公司、苏州棱镜七彩信息科技有限公司、浙江木链物联网科技有限公司、北京升鑫网络科技有限公司、广电奇安网络科技（重庆）有限公司、博智安全科技股份有限公司、湖北珞格科技发展有限公司、巨鹏信息科技有限公司、北京冠程科技有限公司、山东新潮信息技术有限公司、吉林省信睿网络信息安全有限公司、江苏保旺达软件技术有限公司、奇安星城网络安全运营服务（长沙）有限公司、杭州美创科技有限公司、北京机沃科技有限公司、平安银河实验室、浙江安腾信息技术有限公司、北京华云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及其他个人白帽子向 CNVD 提交了 6909 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 5196 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）	3549	3549
奇安信网神（补天平台）	1326	1326
新华三技术有限公司	386	0
上海交大	321	321
深信服科技股份有限公司	310	0
北京神州绿盟科技有限公司	249	7
北京数字观星科技有	232	0

限公司		
安天科技集团股份有限公司	220	0
北京天融信网络安全技术有限公司	136	37
恒安嘉新（北京）科技股份公司	129	0
北京启明星辰信息安全技术有限公司	88	33
远江盛邦（北京）网络安全科技股份有限公司	77	77
杭州安恒信息技术股份有限公司	57	57
京东科技信息技术有限公司	56	34
天津市国瑞数码安全系统股份有限公司	50	0
南京众智维信息科技有限公司	48	48
中国电信集团系统集成有限责任公司	32	2
西安四叶草信息技术有限公司	29	29
北京知道创宇信息技术有限公司	15	0
内蒙古云科数据服务股份有限公司	2	2
南京联成科技发展股份有限公司	1	1
内蒙古奥创科技有限公司	1	1
北京华顺信安科技有限公司	234	2
西门子（中国）有限	45	0

公司		
山石网科通信技术股份有限公司	23	23
河南东方云盾信息技术有限公司	20	20
上海嘉韦思信息技术有限公司	11	11
星云博创科技有限公司	10	10
广州易东信息安全技术有限公司	10	10
苏州棱镜七彩信息科技有限公司	8	8
浙江木链物联网科技有限公司	6	6
北京升鑫网络科技有限公司	5	5
广电奇安网络科技（重庆）有限公司	5	5
博智安全科技股份有限公司	3	3
湖北珞格科技发展有限公司	2	2
巨鹏信息科技有限公司	2	2
北京冠程科技有限公司	2	2
山东新潮信息技术有限公司	1	1
吉林省信睿网络信息安全有限公司	1	1
江苏保旺达软件技术有限公司	1	1
奇安星城网络安全运营服务（长沙）有限	1	1

公司		
杭州美创科技有限公司	1	1
北京机沃科技有限公司	1	1
平安银河实验室	1	1
浙江安腾信息技术有限公司	1	1
北京华云安信息技术有限公司	1	1
河南信安世纪科技有限公司	1	1
思而听网络科技有限公司	1	1
CNCERT 内蒙古分中心	3	3
CNCERT 四川分中心	1	1
个人	1261	1261
报送总计	8976	6909

本周漏洞按类型和厂商统计

本周，CNVD 收录了 474 个漏洞。WEB 应用 153 个，应用程序 142 个，网络设备（交换机、路由器等网络端设备）128 个，智能设备（物联网终端设备）17 个，数据库 16 个，操作系统 11 个，安全产品 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	153
应用程序	142
网络设备（交换机、路由器等网络端设备）	128
智能设备（物联网终端设备）	17
数据库	16
操作系统	11
安全产品	7

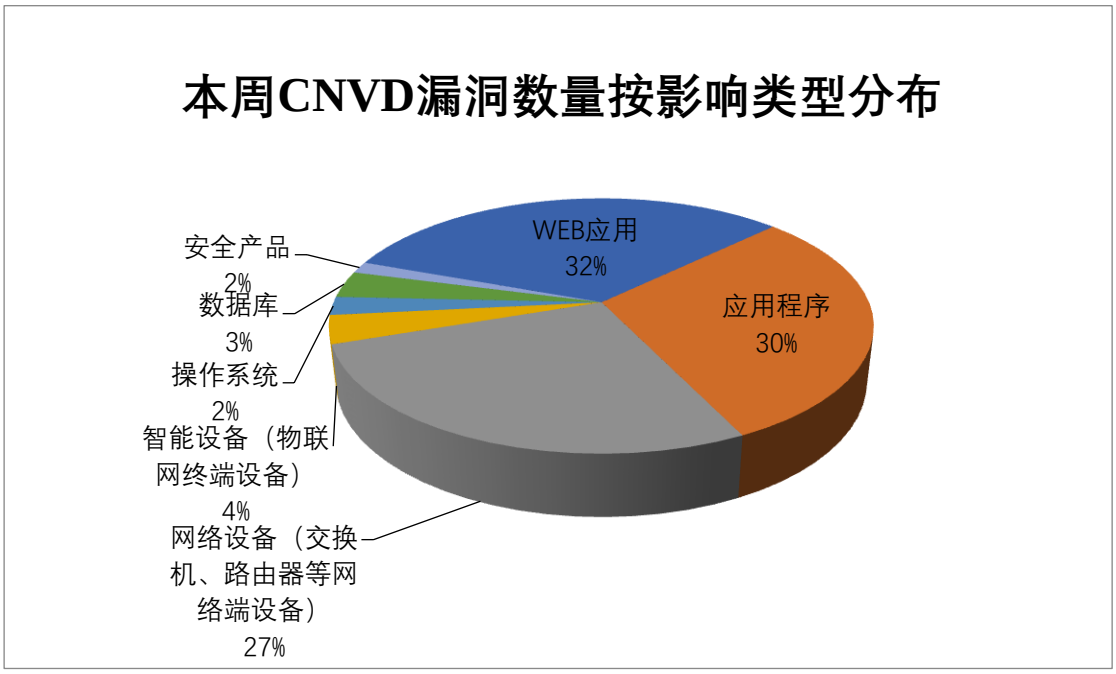

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Siemens、H3C、Apache 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	Siemens	45	9%
2	H3C	20	4%
3	Apache	18	4%
4	IBM	14	3%
5	WordPress	13	3%
6	Linksys	12	3%
7	Adobe	12	3%
8	Tenda	12	3%
9	TOTOLINK	11	2%
10	其他	317	66%

本周行业漏洞收录情况

本周，CNVD 收录了 88 个电信行业漏洞，19 个移动互联网行业漏洞，25 个工控行业漏洞（如下图所示）。其中，“Robustel R1510 操作系统命令注入漏洞（CNVD-2022-51422）、Siemens SIMATIC CP SRCS VPN Feature 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/

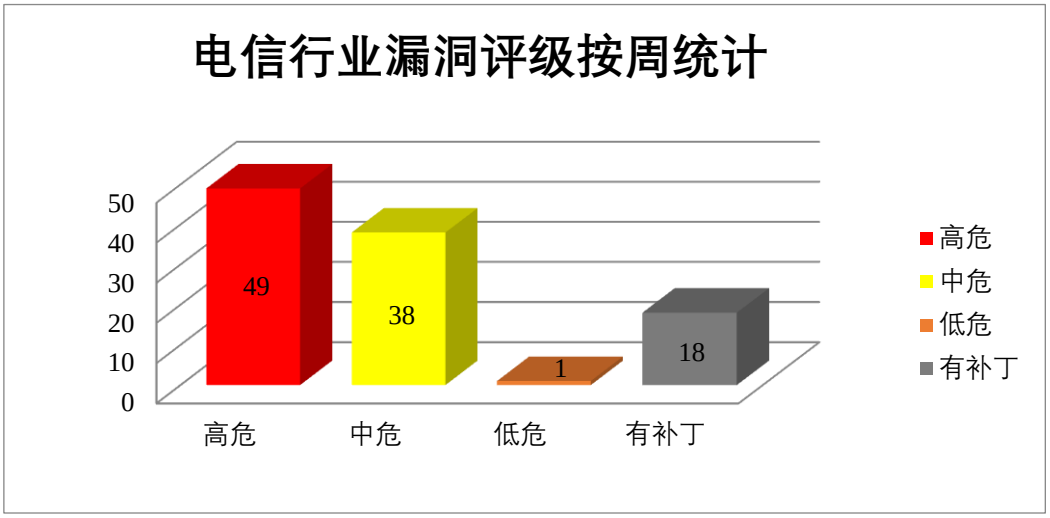

图 3 电信行业漏洞统计

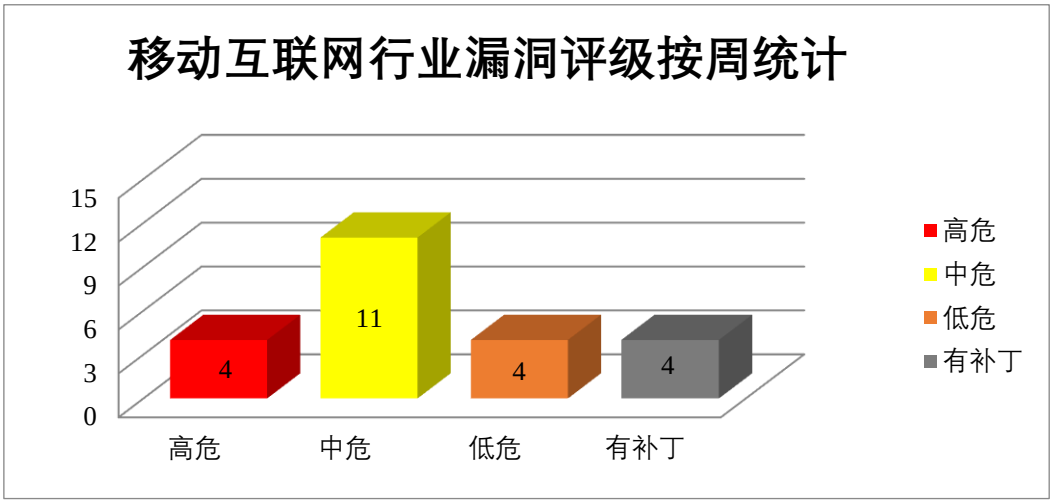

图 4 移动互联网行业漏洞统计

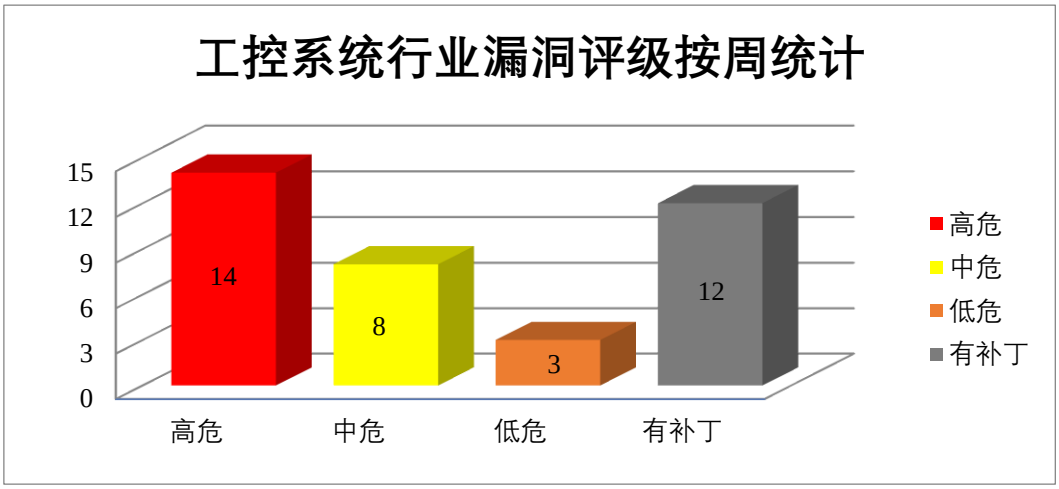

图 5 工控系统行业漏洞统计

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、IBM 产品安全漏洞

IBM Jazz Team Server 是美国 IBM 公司的一个应用服务器。提供了基础服务，这些服务使一组工具可以作为单个逻辑服务器一起工作，并且包括提供工具特定功能的任意数量的 Jazz Team Server Extensions。IBM DB2 是一套关系型数据库管理系统。该系统的执行环境主要有 UNIX、Linux、IBMi、z/OS 以及 Windows 服务器版本。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。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞从系统发送未经授权的请求，可能导致网络枚举或促进其他攻击，信息泄露等。

CNVD 收录的相关漏洞包括：IBM Jazz Team Server 服务器端请求伪造漏洞（CNVD-2022-51652、CNVD-2022-51654）、IBM DB2 信息泄露漏洞（CNVD-2022-51656）、IBM DB2 拒绝服务漏洞（CNVD-2022-51655）、IBM Jazz Team Server 信息泄露漏洞（CNVD-2022-51653、CNVD-2022-51660）、IBM Jazz Team Server 点击劫持漏洞、IBM Spectrum Copy Data Management 信息泄露漏洞（CNVD-2022-51662）。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-2022-51652
https://www.cnvd.org.cn/flaw/show/CNVD-2022-51656
https://www.cnvd.org.cn/flaw/show/CNVD-2022-51655
https://www.cnvd.org.cn/flaw/show/CNVD-2022-51654
https://www.cnvd.org.cn/flaw/show/CNVD-2022-51653
https://www.cnvd.org.cn/flaw/show/CNVD-2022-51660
https://www.cnvd.org.cn/flaw/show/CNVD-2022-51657
https://www.cnvd.org.cn/flaw/show/CNVD-2022-51662

2、Apache 产品安全漏洞

Apache SystemDS 是美国阿帕奇（Apache）基金会的用于端到端数据科学生命周期的开源机器学习系统。Apache NiFi 是一套数据处理和分发系统。该系统主要用于数据路由、转换和系统中介逻辑。Apache NiFi Registry 是其中的一个用于存储和管理版本化流程的注册表。Apache Hadoop 是一套开源的分布式系统基础架构。该产品能够对大量数据进行分布式处理，并具有高可靠性、高扩展性、高容错性等特点。Apache Flume 是一种分布式、可靠且可用的服务。用于高效收集、聚合和移动大量日志数据。Apache HTTP Server 是一款开源网页服务器。该服务器具有快速、可靠且可通过简单的 API 进行扩充的特点。Apache Archiva 是一套用于管理一个或多个远程存储的软件。该软件

提供远程 Repository 代理、基于角色的安全访问管理和使用情况报告等功能。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞在 Linux 和 macOS 平台上注入操作系统命令，导致 yarn 级别的用户可能以 root 用户身份执行任意命令等。

CNVD 收录的相关漏洞包括：Apache SystemDS 拒绝服务漏洞、Apache NiFi 命令注入漏洞、Apache Hadoop 权限提升漏洞（CNVD-2022-51055）、Apache Flume 远程代码执行漏洞、Apache HTTP Server 信息泄露漏洞（CNVD-2022-51060）、Apache HTTP Server HTTP 请求走私漏洞、Apache Hadoop 缓冲区溢出漏洞（CNVD-2022-51057）、Apache Archiva 安全特征问题漏洞。其中，“Apache Hadoop 权限提升漏洞（CNVD-2022-51055）、Apache Flume 远程代码执行漏洞、Apache Hadoop 缓冲区溢出漏洞（CNVD-2022-51057）”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-2022-51052
https://www.cnvd.org.cn/flaw/show/CNVD-2022-51056
https://www.cnvd.org.cn/flaw/show/CNVD-2022-51055
https://www.cnvd.org.cn/flaw/show/CNVD-2022-51054
https://www.cnvd.org.cn/flaw/show/CNVD-2022-51060
https://www.cnvd.org.cn/flaw/show/CNVD-2022-51058
https://www.cnvd.org.cn/flaw/show/CNVD-2022-51057
https://www.cnvd.org.cn/flaw/show/CNVD-2022-51062

3、SAP 产品安全漏洞

SAP 3D Visual Enterprise Viewer 是德国思爱普（SAP）公司的一款 3D 视图查看器。该软件支持在所有行业标准的桌面应用中发布 2D、3D 场景，并支持以独立可执行程序和 ActiveX 空间单独安装。SAP PowerDesigner 是德国思爱普（SAP）公司的一款数据库设计软件。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞绕过系统的根磁盘访问限制，在系统磁盘根路径上写入或创建程序文件，并提升应用程序的权限，导致应用程序崩溃并且用户暂时无法使用，直到重新启动应用程序等。

CNVD 收录的相关漏洞包括：SAP 3D Visual Enterprise Viewer 输入验证错误漏洞（CNVD-2022-50937、CNVD-2022-50936、CNVD-2022-50940、CNVD-2022-50939、CNVD-2022-50938、CNVD-2022-50942、CNVD-2022-50941）、SAP PowerDesigner 代码问题漏洞。其中，“SAP PowerDesigner 代码问题漏洞”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-2022-50937
https://www.cnvd.org.cn/flaw/show/CNVD-2022-50936
https://www.cnvd.org.cn/flaw/show/CNVD-2022-50940

https://www.cnvd.org.cn/flaw/show/CNVD-2022-50939

https://www.cnvd.org.cn/flaw/show/CNVD-2022-50938

https://www.cnvd.org.cn/flaw/show/CNVD-2022-50942

https://www.cnvd.org.cn/flaw/show/CNVD-2022-50941

https://www.cnvd.org.cn/flaw/show/CNVD-2022-50943

4、Fortinet 产品安全漏洞

Fortinet FortiGate 是美国飞塔（Fortinet）公司的一套网络安全平台。该平台提供防火墙、防病毒和入侵防御（IPS）、应用控制、反垃圾邮件、无线控制器和广域网加速等功能。FortiSOAR 是一种安全编排、自动化和响应 (SOAR) 解决方案。Fortinet Forti Proxy SSL VPN 是一个应用软件。提供了一个入侵检测功能。Fortinet FortiOS 是一套专用于 FortiGate 网络安全平台上的安全操作系统。该系统为用户提供防火墙、防病毒、IPSec/SSLVPN、Web 内容过滤和反垃圾邮件等多种安全功能。Fortinet FortiWLC 是一款无线局域网控制器。Fortinet FortiPortal 是 FortiGate、FortiWiFi 和 FortiAP 产品线的高级、功能丰富的托管安全分析和管理支持工具，可作为虚拟机供 MSP 使用。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞窃取潜在的敏感信息，更改网页的外观，执行网络钓鱼和偷渡式下载攻击，绕过已实施的安全限制，获取对网关 API 数据的未经授权的访问等。

CNVD 收录的相关漏洞包括：Fortinet FortiGate 跨站脚本漏洞（CNVD-2022-50950）、Fortinet FortiSOAR 访问控制错误漏洞、Fortinet FortiProxy SSL VPN 跨站脚本漏洞、Fortinet FortiOS 信息泄露漏洞（CNVD-2022-50947）、Fortinet FortiWLM SQL 注入漏洞（CNVD-2022-50953）、Fortinet FortiWLM 路径遍历漏洞、Fortinet FortiPortal 安全特征问题漏洞、Fortinet FortiGate 输入验证错误漏洞。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-2022-50950

https://www.cnvd.org.cn/flaw/show/CNVD-2022-50949

https://www.cnvd.org.cn/flaw/show/CNVD-2022-50948

https://www.cnvd.org.cn/flaw/show/CNVD-2022-50947

https://www.cnvd.org.cn/flaw/show/CNVD-2022-50953

https://www.cnvd.org.cn/flaw/show/CNVD-2022-50952

https://www.cnvd.org.cn/flaw/show/CNVD-2022-50955

https://www.cnvd.org.cn/flaw/show/CNVD-2022-50954

5、Huawei HarmonyOS 权限管理不当漏洞

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。本周，Huawei HarmonyOS 被披露存在权限管理不当漏洞。攻击者利用该漏洞可导致获取 CPLC 信息。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-2022-51605

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-2022-50668	Cisco Secure Network Analytics 远程代码执行漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-stealth-rce-2hYb9KFK
CNVD-2022-50943	SAP PowerDesigner 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://launchpad.support.sap.com/#/notes/3197005
CNVD-2022-51055	Apache Hadoop 权限提升漏洞（CNVD-2022-51055）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://lists.apache.org/thread/ctr84rmo3xd2tzqcx2b277c8z692vhl5
CNVD-2022-51054	Apache Flume 远程代码执行漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://lists.apache.org/thread/16nf6b81zjpdc4y93ho99oxo83ddbsvg
CNVD-2022-51423	Robustel R1510 操作系统命令注入漏洞（CNVD-2022-51423）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://talosintelligence.com/vulnerability_reports/TALOS-2022-1573
CNVD-2022-51427	Robustel R1510 命令执行漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://talosintelligence.com/vulnerability_reports/TALOS-2022-1570
CNVD-2022-51439	Siemens SCALANCE X Switches 缓冲区溢出漏洞	高	用户可参考如下供应商提供的安全公告获得补丁信息：https://cert-portal.siemens.com/productcert/html/ssa-310038.html
CNVD-2022-51445	Nodejs Dll 劫持漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://nodejs.org/en/
CNVD-2022-51616	Siemens PADS Standard/Plus Viewer 越界读取漏洞（CNVD-2022-51616）	高	用户可参考如下供应商提供的安全公告获得补丁信息：https://cert-portal.siemens.com/productcert/html/ssa-439148.html

CNVD-2022-51629	Siemens Teamcenter Visualization and JT2Go 缓冲区溢出漏洞	高	用户可参考如下供应商提供的安全公告获得补丁信息：https://cert-portal.siemens.com/productcert/html/ssa-829738.html

小结：本周，IBM 产品被披露存在多个漏洞，攻击者可利用漏洞从系统发送未经授权的请求，可能导致网络枚举或促进其他攻击，信息泄露等。此外，Apache、SAP、Fortinet 等多款产品被披露存在多个漏洞，攻击者可利用漏洞窃取潜在的敏感信息，更改网页的外观，绕过系统的根磁盘访问限制，在系统磁盘根路径上写入或创建程序文件，并提升应用程序的权限，在 Linux 和 macOS 平台上注入操作系统命令。另外，HarmonyOS 被披露存在权限管理不当漏洞。攻击者可利用漏洞导致获取 CPLC 信息。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、TOTOLINK N600R 缓冲区溢出漏洞

验证描述

TOTOLINK N600R 是中国台湾吉翁电子（TOTOLINK）公司的一款无线路由器。

TOTOLINK N600R V4.3.0cu.7647_B20210106 版本存在缓冲区溢出漏洞，该漏洞源于 FUN_004200c8 函数中的注释参数缺乏长度验证，攻击者可利用该漏洞导致缓冲区溢出。

验证信息

POC 链接：https://github.com/d1tto/IoT-vuln/tree/main/Totolink/5.setStaticDhcpConfig

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2022-50677

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. VMware 修补了 11 月披露的 vCenter Server 漏洞

在披露 vCenter Server 的 IWA（集成 Windows 身份验证）机制中的提权漏洞八个月后，VMware 发布了针对其中一个受影响版本的补丁。

参考链接：https://www.bleepingcomputer.com/news/security/vmware-patches-vcenter-server-flaw-disclosed-in-november/

2. 微软修复了数十个 Azure Site Recovery 权限提升错误

Microsoft 已修复 Azure Site Recovery 套件中的 32 个漏洞，这些漏洞可能允许攻击者获得提升的权限或执行远程代码执行。

参考链接：https://www.bleepingcomputer.com/news/security/microsoft-fixes-dozens-of-azure-site-recovery-privilege-escalation-bugs/

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