国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2022 年 02 月 14 日-2022 年 02 月 20 日 **2022 年第 7 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 497 个，其中高危漏洞 153 个、中危漏洞 320 个、低危漏洞 24 个。漏洞平均分值为 6.07。本周收录的漏洞中，涉及 0day 漏洞 195 个（占 39%），其中互联网上出现“Saraban 文件上传漏洞、Saraban 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事件型漏洞总数 4976 个，与上周（2382 个）环比增加 109%。

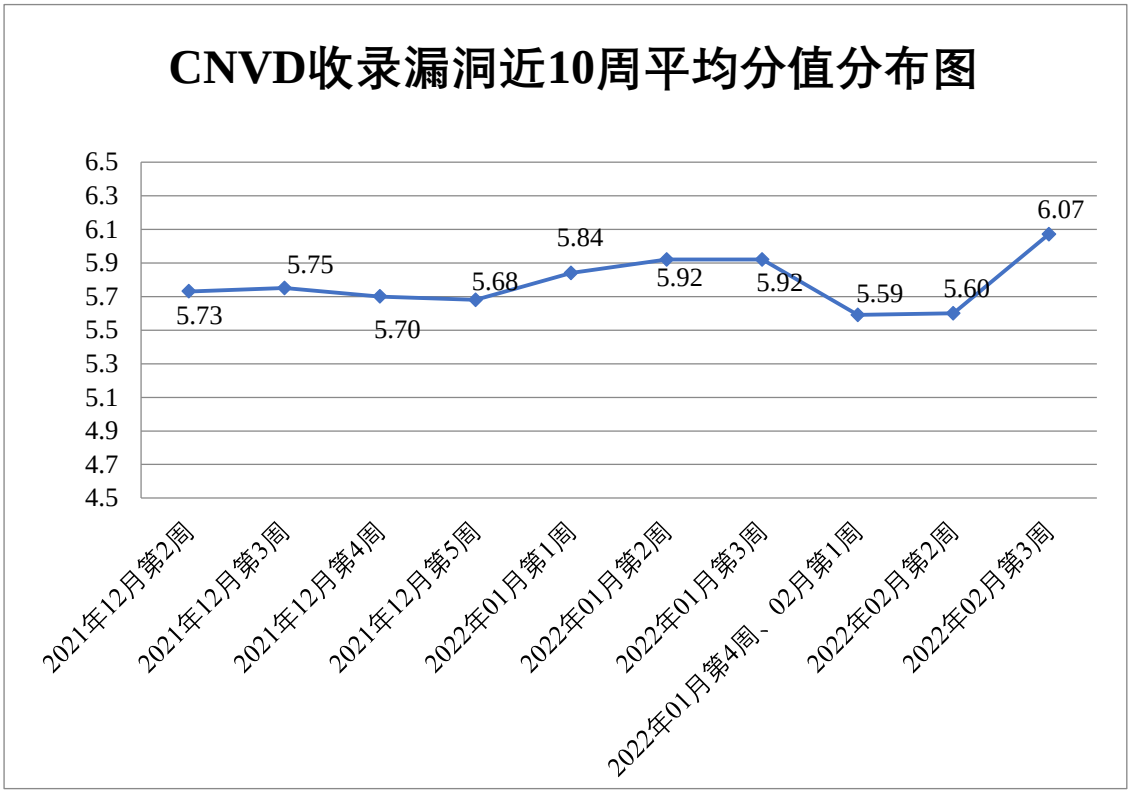

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 39 起，向基础电信企业通报漏洞事件 40 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 718 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 43 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 89 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：

珠海金山办公软件有限公司、重庆森鑫炬科技有限公司、中企动力科技股份有限公司、正方软件股份有限公司、镇江市云优网络科技有限公司、浙江臻善科技股份有限公司、浙江宇视科技有限公司、浙江大华技术股份有限公司、长沙友点软件科技有限公司、长沙米拓信息技术有限公司、漳州豆壳网络科技有限公司、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）办公系统有限公司、武汉达梦数据库股份有限公司、温州互引信息技术有限公司、微软（中国）有限公司、苏州科达科技股份有限公司、松下电器（中国）有限公司、四创科技有限公司、思科系统（中国）网络技术有限公司、世邦通信股份有限公司、深圳市普燃计算机软件科技有限公司、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、深圳科士达科技股份有限公司、深圳警翼智能科技股份有限公司、深圳奥联信息安全技术有限公司、上海卓卓网络科技有限公司、上海云翌通信科技有限公司、上海焱凤信息技术有限公司、上海居亦科技发展有限公司、上海方正信息安全技术有限公司、上海博达数据通信有限公司、上海冰峰计算机网络技术有限公司、上海贝锐信息科技股份有限公司、上海安达通信息安全技术股份有限公司、上海爱数信息技术股份有限公司、陕西西咸新区公共交通集团有限公司、山西先启科技有限公司、山脉科技股份有限公司、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、锐捷网络股份有限公司、任子行网络技术股份有限公司、青岛海尔生物医疗股份有限公司、金蝶软件（中国）有限公司、江西铭软科技有限公司、佳能（中国）有限公司、济南卓源软件有限公司、吉翁电子（深圳）有限公司、惠普贸易（上海）有限公司、湖南奥科网络技术股份有限公司、杭州雄伟科技开发股份有限公司、杭州海康威视数字技术股份有限公司、杭州飞致云信息科技有限公司、广州易神软件科技有限公司、广州易全信息科技有限公司、广州同鑫科技有限公司、广州添富信息科技有限公司、广州市溢信科技股份有限公司、广州酷狗计算机科技有限公司、广州安网通信技术有限公司、福州网钛软件科技有限公司、福建星网锐捷通讯股份有限公司、福建省海峡信息技术有限公司、东莞市光速网络技术有限公司、戴尔(中国)有限公司、北京亚控科技发展有限公司、北京星网锐捷网络技术有限公司、北京文网亿联科技有限公司、北京通王科技有限公司、北京数科网维技术有限责任公司、北京圣博润高新技术股份有限公司、北京米尔伟业科技有限公司、北京立

思辰科技股份有限公司、北京康邦科技有限公司、北京九思协同软件有限公司、北京金和网络股份有限公司、北京环球慧爽科技有限公司、北京华富远科技术有限公司、北京棣南新宇科技有限公司、北京百卓网络技术有限公司、北京安博通科技股份有限公司、安徽青柿信息科技有限公司、施耐德电气、梦想 CMS、VeryPDF、TOTOLINK、TaoCMS、SEMCMS、Sapido、Projectworlds、phpwind、OwnCloud、MOBOTIX、HuCart、Glyph & Cog, LLC、emlog、cszcms、Cesanta 和 catfishcms。

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、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、杭州安恒信息技术股份有限公司、北京神州绿盟科技有限公司等单位报送公开收集的漏洞数量较多。天津偕行科技有限公司、山东云天安全技术有限公司、南京树安信息技术有限公司、广东蓝爵网络安全技术股份有限公司、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、长春嘉诚信息技术股份有限公司、北京安华金和科技有限公司、苏州棱镜七彩信息科技有限公司、河南灵创电子科技有限公司、华鲁数智信息技术（北京）有限公司、开元华创科技（集团）有限公司、杭州默安科技有限公司、北京网御星云信息技术有限公司、亚信科技（成都）有限公司、山东新潮信息技术有限公司、山石网科通信技术股份有限公司、北方实验室（沈阳）股份有限公司、河南信安世纪科技有限公司、智网安云（武汉）信息技术有限公司、贵州泰若数字科技有限公司、博智安全科技股份有限公司、武汉安域信息安全技术有限公司、上海纽盾科技股份有限公司、中电云数智科技有限公司、广州百蕴启辰科技有限公司、上海上讯信息技术股份有限公司、深圳昂楷科技有限公司、南京禾盾信息科技有限公司、泰山信息科技有限公司、内蒙古洞明科技有限公司、北京机沃科技有限公司、北京华云安信息技术有限公司、广西塔易信息技术有限公司、海南神州希望网路有限公司、杭州美创科技有限公司、中通服创发科技有限责任公司、中安网盾（广州）信息科技有限公司、济南时代确信信息安全测评有限公司及其他个人白帽子向 CNVD 提交了 4976 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 2406 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）	1475	1475
上海交大	490	490
奇安信网神（补天平台）	441	441
新华三技术有限公司	326	0

安天科技集团股份有限公司	223	0
北京天融信网络安全技术有限公司	202	57
杭州安恒信息技术股份有限公司	196	73
北京神州绿盟科技有限公司	127	8
恒安嘉新（北京）科技股份公司	119	0
天津市国瑞数码安全系统股份有限公司	86	0
北京启明星辰信息安全技术有限公司	67	10
北京数字观星科技有限公司	53	0
南京众智维信息科技有限公司	42	42
远江盛邦（北京）网络安全科技股份有限公司	41	41
中国电信集团系统集成有限责任公司	29	0
西安四叶草信息技术有限公司	24	24
内蒙古云科数据服务股份有限公司	23	23
南京联成科技发展股份有限公司	12	12
深信服科技股份有限公司	5	0
北京知道创宇信息技术股份有限公司	3	0
北京智游网安科技有	1	1

限公司		
深圳市腾讯计算机系统有限公司（玄武实验室）	1	1
北京华顺信安科技有限公司	107	0
天津偕行科技有限公司	56	56
山东云天安全技术有限公司	50	50
南京树安信息技术有限公司	42	42
联想集团	35	0
广东蓝爵网络安全技术股份有限公司	34	34
北京山石网科信息技术有限公司	33	33
重庆都会信息科技有限公司	31	31
杭州迪普科技股份有限公司	29	0
长春嘉诚信息技术股份有限公司	20	20
北京安华金和科技有限公司	18	18
苏州棱镜七彩信息科技有限公司	17	17
河南灵创电子科技有限公司	16	16
华鲁数智信息技术（北京）有限公司	15	15
开元华创科技（集团）有限公司	13	13
杭州默安科技有限公	10	10

司		
北京网御星云信息技术有限公司	10	10
亚信科技（成都）有限公司	7	1
山东新潮信息技术有限公司	4	4
山石网科通信技术股份有限公司	3	3
北方实验室（沈阳）股份有限公司	3	3
河南信安世纪科技有限公司	3	3
智网安云（武汉）信息技术有限公司	3	3
贵州泰若数字科技有限公司	3	3
博智安全科技股份有限公司	2	2
武汉安域信息安全技术有限公司	2	2
上海纽盾科技股份有限公司	2	2
中电云数智科技有限公司	1	1
广州百蕴启辰科技有限公司	1	1
上海上讯信息技术股份有限公司	1	1
深圳昂楷科技有限公司	1	1
南京禾盾信息科技有限公司	1	1
泰山信息科技有限公	1	1

司		
内蒙古洞明科技有限公司	1	1
北京机沃科技有限公司	1	1
北京华云安信息技术有限公司	1	1
广西塔易信息技术有限公司	1	1
海南神州希望网路有限公司	1	1
杭州美创科技有限公司	1	1
中通服创发科技有限责任公司	1	1
中安网盾（广州）信息科技有限公司	1	1
济南时代确信信息安全测评有限公司	1	1
CNCERT 四川分中心	5	5
CNCERT 河北分中心	1	1
个人	1869	1866
报送总计	6444	4976

本周漏洞按类型和厂商统计

本周，CNVD 收录了 497 个漏洞。应用程序 227 个，WEB 应用 143 个，智能设备（物联网终端设备）60 个，网络设备（交换机、路由器等网络端设备）56 个，操作系统 5 个，数据库 5 个，安全产品 1 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	227
WEB 应用	143
智能设备（物联网终端设备）	60
网络设备（交换机、路由器等网络端设备）	56
操作系统	5

数据库	5
安全产品	1

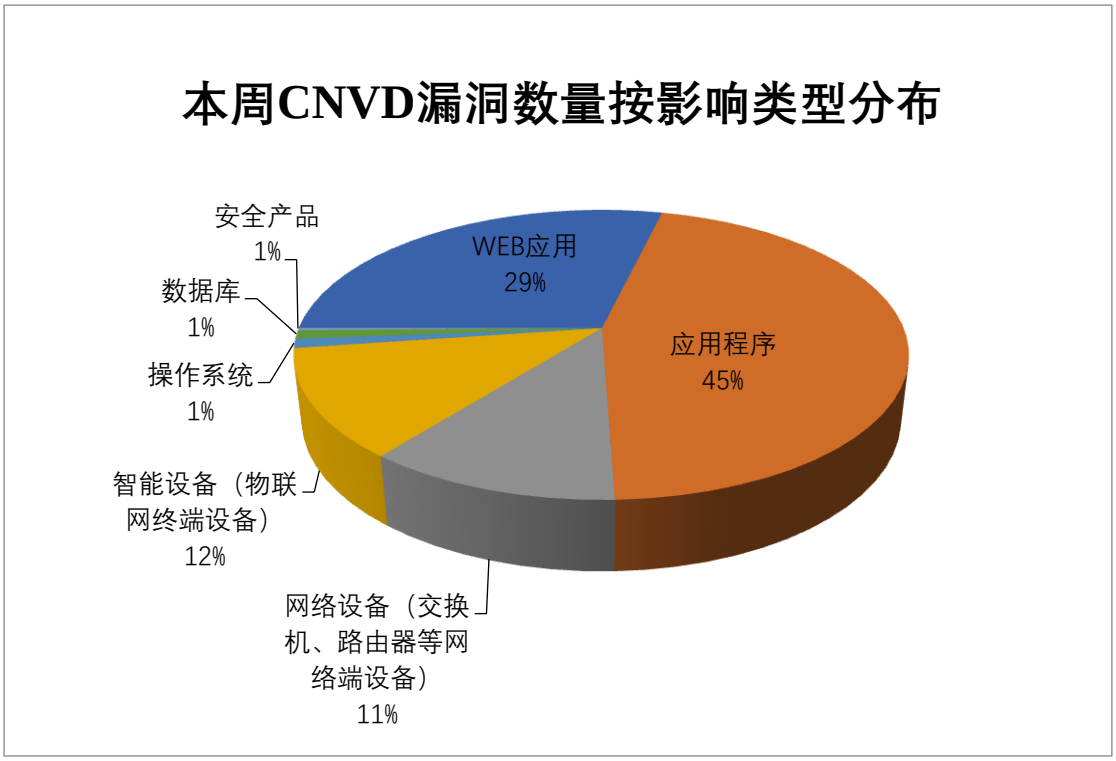

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Jsish、Reolink、Tenda 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	Jsish	43	9%
2	Reolink	40	8%
3	Tenda	27	5%
4	Siemens	26	5%
5	Insyde	24	5%
6	Adobe	21	4%
7	四创科技有限公司	21	4%
8	Jerry	18	4%
9	Wireshark	16	3%
10	其他	261	53%

本周行业漏洞收录情况

本周，CNVD 收录了 40 个电信行业漏洞，12 个移动互联网行业漏洞，13 个工控行

业漏洞（如下图所示）。其中，“D-Link DIR-X1860 拒绝服务漏洞（CNVD-2022-11517）、HUAWEI EMUI 缓冲区溢出漏洞（CNVD-2022-12766）、Tenda G1 and G3 操作系统命令注入漏洞”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/

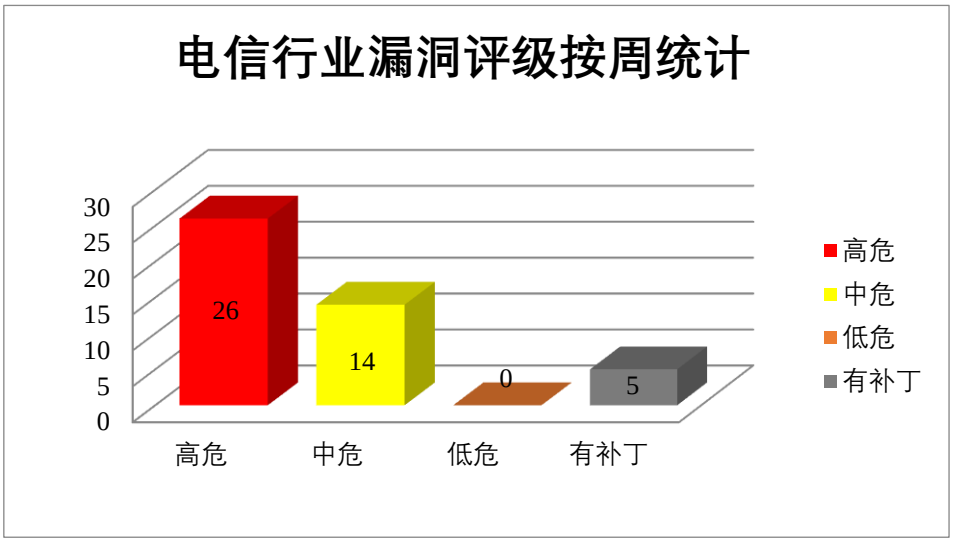

图 3 电信行业漏洞统计

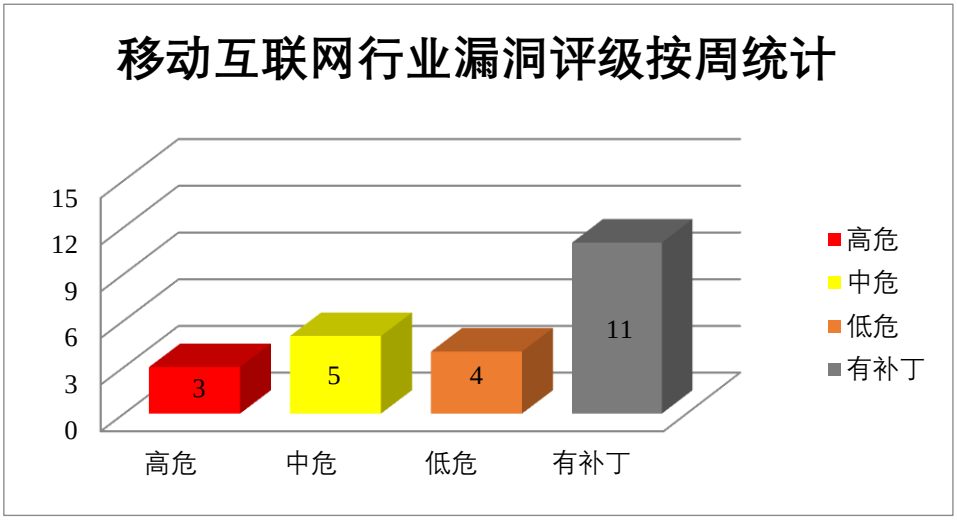

图 4 移动互联网行业漏洞统计

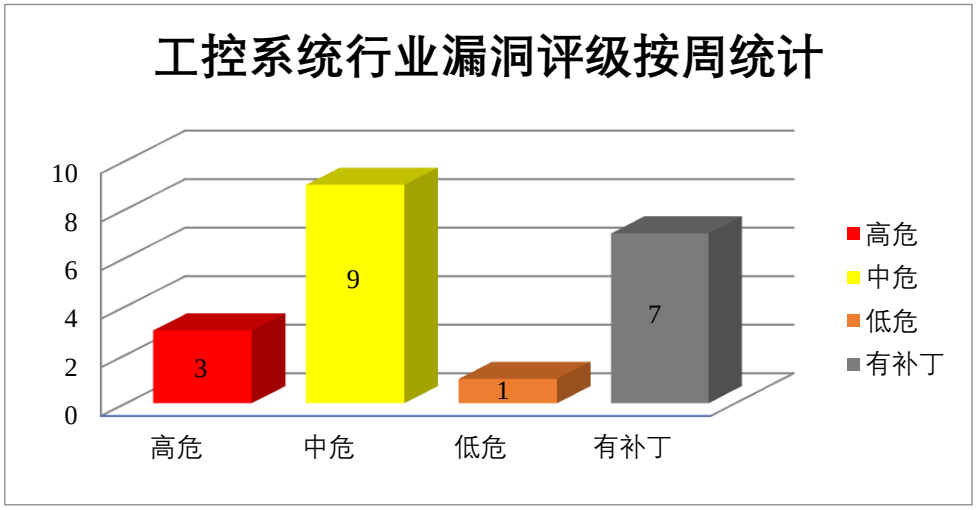

图 5 工控系统行业漏洞统计

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、 Adobe 产品安全漏洞

Adobe Acrobat Reader Dc 是美国 Adobe 公司的一个 Pdf 阅读工具。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞执行任意代码。

CNVD 收录的相关漏洞包括：Adobe Acrobat Reader Dc 缓冲区溢出漏洞（CNVD-2022-11149、CNVD-2022-11148、CNVD-2022-11156、CNVD-2022-11155、CNVD-2022-10759、CNVD-2022-10760）、Adobe Acrobat Reader Dc 越界写入漏洞（CNVD-2022-10757）、Adobe Acrobat Reader DC 整数溢出漏洞。其中，除“Adobe Acrobat Reader Dc 缓冲区溢出漏洞（CNVD-2022-11148、CNVD-2022-11156、CNVD-2022-11155）”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-2022-11149

https://www.cnvd.org.cn/flaw/show/CNVD-2022-11148

https://www.cnvd.org.cn/flaw/show/CNVD-2022-11156

https://www.cnvd.org.cn/flaw/show/CNVD-2022-11155

https://www.cnvd.org.cn/flaw/show/CNVD-2022-10759

https://www.cnvd.org.cn/flaw/show/CNVD-2022-10760

https://www.cnvd.org.cn/flaw/show/CNVD-2022-10757

https://www.cnvd.org.cn/flaw/show/CNVD-2022-10760

2、 Wireshark 产品安全漏洞

Wireshark（前称 Ethereal）是 Wireshark 团队的一套网络数据包分析软件。该软件

的功能是截取网络数据包，并显示出详细的数据以供分析。Gryphon dissector 是其中的一个 Gryphon 协议解析器。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞执行拒绝服务攻击。

CNVD 收录的相关漏洞包括：Wireshark 拒绝服务漏洞（CNVD-2022-11189）、Wireshark RTMPT 解析器拒绝服务漏洞、Wireshark Sysdig 事件解析器拒绝服务漏洞、Wireshark BitTorrent DHT 解析器拒绝服务漏洞、Wireshark 输入验证错误漏洞（CNVD-2022-11204、CNVD-2022-11203、CNVD-2022-11202、CNVD-2022-11206）。其中“Wireshark 拒绝服务漏洞（CNVD-2022-11189）”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-2022-11189
https://www.cnvd.org.cn/flaw/show/CNVD-2022-11200
https://www.cnvd.org.cn/flaw/show/CNVD-2022-11199
https://www.cnvd.org.cn/flaw/show/CNVD-2022-11198
https://www.cnvd.org.cn/flaw/show/CNVD-2022-11204
https://www.cnvd.org.cn/flaw/show/CNVD-2022-11203
https://www.cnvd.org.cn/flaw/show/CNVD-2022-11202
https://www.cnvd.org.cn/flaw/show/CNVD-2022-11206

3、Microsoft 产品安全漏洞

Microsoft Windows Update Assistant 是美国微软（Microsoft）公司的一款系统更新工具。Microsoft Windows Print Spooler 是美国微软（Microsoft）公司的一个打印后台处理程序组件。Microsoft Edge 是美国微软（Microsoft）公司的一款 Windows 10 之后版本系统附带的 Web 浏览器。Microsoft Edge for Android 是美国微软（Microsoft）公司的一款适配 Android 系统的 Web 浏览器。Microsoft Windows 是一款由美国微软公司开发的窗口化操作系统。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞获取敏感信息，删除系统上的目标文件，提升权限，使用 SYSTEM 权限运行任意代码等。

CNVD 收录的相关漏洞包括：Microsoft Windows Update Assistant 权限提升漏洞、Microsoft Windows Print Spooler 远程代码执行漏洞（CNVD-2022-10026、CNVD-2022-10025）、Microsoft Edge (Chromium-based)权限提升漏洞、Microsoft Edge 欺骗漏洞（CNVD-2022-10027）、Microsoft Edge for Android 信息泄露漏洞、Microsoft Windows IKE Extension 拒绝服务漏洞（CNVD-2022-10030、CNVD-2022-10031）。其中“Microsoft Windows Print Spooler 远程代码执行漏洞（CNVD-2022-10025）、Microsoft Windows IKE Extension 拒绝服务漏洞”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-2022-10024
https://www.cnvd.org.cn/flaw/show/CNVD-2022-10026
https://www.cnvd.org.cn/flaw/show/CNVD-2022-10025
https://www.cnvd.org.cn/flaw/show/CNVD-2022-10028
https://www.cnvd.org.cn/flaw/show/CNVD-2022-10027
https://www.cnvd.org.cn/flaw/show/CNVD-2022-10029
https://www.cnvd.org.cn/flaw/show/CNVD-2022-10030
https://www.cnvd.org.cn/flaw/show/CNVD-2022-10031

4、Siemens 产品安全漏洞

Siemens Simcenter Femap 是德国西门子（Siemens）公司的一款尖端工程学仿真应用程序。用于创建、编辑和导入/重用复杂产品或系统基于网格的有限元分析模型。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进程的上下文中执行代码。

CNVD 收录的相关漏洞包括：Siemens Simcenter Femap 堆栈缓冲区溢出漏洞（CNVD-2022-10011、CNVD-2022-10015、CNVD-2022-10014）、Siemens Simcenter Femap 越界写入漏洞（CNVD-2022-10010、CNVD-2022-10009、CNVD-2022-10013）、Siemens Simcenter Femap 内存破坏漏洞（CNVD-2022-10012、CNVD-2022-10016）。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-2022-10011
https://www.cnvd.org.cn/flaw/show/CNVD-2022-10015
https://www.cnvd.org.cn/flaw/show/CNVD-2022-10014
https://www.cnvd.org.cn/flaw/show/CNVD-2022-10010
https://www.cnvd.org.cn/flaw/show/CNVD-2022-10009
https://www.cnvd.org.cn/flaw/show/CNVD-2022-10013
https://www.cnvd.org.cn/flaw/show/CNVD-2022-10012
https://www.cnvd.org.cn/flaw/show/CNVD-2022-10016

5、Tenda Ax3 缓冲区溢出漏洞（CNVD-2022-11183）

Tenda Ax3 是中国腾达（Tenda）公司的一款 Ax1800 千兆端口双频 Wifi 6 无线路由器。本周，Tenda AX3 被披露存在缓冲区溢出漏洞，攻击者可利用该漏洞通过 rebootTime 参数造成拒绝服务 (DoS)。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-2022-11183

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-2022-09994	WordPress Perfect Survey 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/c1620905-7c31-4e62-80f5-1d9635be11ad
CNVD-2022-10707	Advantech 信任管理问题漏洞	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://www.advantech.com/support
CNVD-2022-10739	Froxlor 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://github.com/Froxlor/Froxlor/commit/eb592340b022298f62a0a3e8450dbfbe29585782
CNVD-2022-10745	Apache Dubbo 格式化字符串错误漏洞	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.html/r40212261fd5d638074b65f22ac73eebe93ace310c79d4cfcca4863da%40%3Cdev.dubbo.apache.org%3E
CNVD-2022-11102	PrinterLogic Web Stack 服务器端请求伪造漏洞	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.printerlogic.com/security-bulletin/
CNVD-2022-11209	Tensorflow 输入验证错误漏洞（CNVD-2022-11209）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/tensorflow/tensorflow/security/advisories/GHSA-8jj7-5vxc-pg2q
CNVD-2022-11499	Talkyard 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://www.whitesourcesoftware.com/vulnerability-database/CVE-2021-25981
CNVD-2022-11517	D-Link DIR-X1860 拒绝服务漏洞（CNVD-2022-11517）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10283
CNVD-2022-11521	Cisco Umbrella 信息泄露漏洞	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://tools.cisco.com/security/center

			/content/CiscoSecurityAdvisory/cisco-sa-swg-fbyps-3z4qT7p
CNVD-2022-11527	Victor CMS posts.php 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/Nguyen-Trung-Kien/CVE/blob/main/CVE-2021-46458/CVE-2021-46458.pdf

小结：本周，Adobe 产品被披露存在多个漏洞，攻击者可利用漏洞执行任意代码。此外，Wireshark、Microsoft、Siemens 等多款产品被披露存在多个漏洞，攻击者可利用漏洞获取敏感信息，删除系统上的目标文件，提升权限，在当前进程的上下文中执行代码等。另外，Tenda Ax3 被披露存在缓冲区溢出漏洞，攻击者可利用该漏洞通过 rebootTime 参数造成拒绝服务 (DoS)。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、Saraban 文件上传漏洞

验证描述

Saraban 是泰国 Softvibe 公司的一个文件管理系统。用于传输文件，通知减少不必要的重复。

Saraban 存在文件上传漏洞，该漏洞源于应用程序的文件上传功能未正确进行访问控制和文件类型限制，攻击者可利用该漏洞上传具有任何文件扩展名的文件，导致任意代码执行。

验证信息

POC 链接：https://orangeo.tech/post/2021/12/24/First-CVEs.html

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2022-10768

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. Apache Cassandra 数据库曝出高危级 RCE 安全漏洞

日前，JFrog 的研究人员披露在 Apache Cassandra 数据库中发现高严重性安全漏洞

（CVE-2021-44521），如果不加以解决，该漏洞可帮助恶意人员在受影响的计算设备上获得远程代码执行（RCE）权限。

参考链接：https://www.aqniu.com/industry/80965.html

2. Argo CD 漏洞泄露 Kubernetes 敏感信息

Argo CD 是一个主流的、开源、持续交付（Continuous Delivery）平台，被广泛应用于 Kubernetes 的声明性 GitOps 连续交付。Apiiro 安全研究人员在 Argo CD 平台中发现了一个 0 day 漏洞，漏洞 CVE 变化为 CVE-2022-24348，CVSS 评分为 7.7 分。该漏洞是一个路径遍历漏洞，攻击者利用该漏洞可以实现权限提升、信息泄露和进一步攻击。

参考链接：https://www.4hou.com/posts/vLy8

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