国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2022 年 01 月 03 日-2022 年 01 月 09 日 **2022 年第 1 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 353 个，其中高危漏洞 103 个、中危漏洞 220 个、低危漏洞 30 个。漏洞平均分值为 5.84。本周收录的漏洞中，涉及 0day 漏洞 229 个（占 65%），其中互联网上出现“Redisgraph Online-matrimonial-project-in-php 文件上传漏洞、projectworlds car rental management system 跨站脚本漏洞”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 3412 个，与上周（36493 个）环比减少 91%。

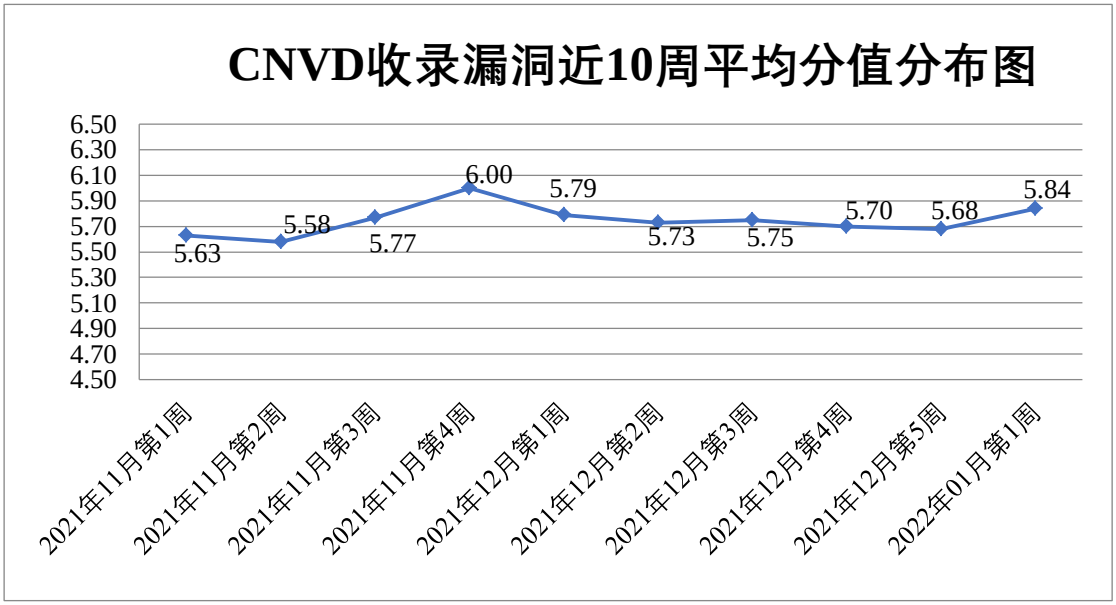

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 38 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 336 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 52 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、重庆本易软件有限公司、正方软件股份有限公司、浙江中控技术股份有限公司、浙江浙大中控信息技术有限公司、浙江宇视科技有限公司、浙江和达科技股份有限公司、友讯电子设备（上海）有限公司、用友网络科技股份有限公司、央视国际网络有限公司、兄弟（中国）商业有限公司、星衍股份有限公司、新天科技股份有限公司、温州互引信息技术有限公司、网神信息技术(北京)股份有限公司、网件（北京）网络技术有限公司、天闻数媒科技(北京)有限公司、苏州天一信德环保科技有限公司、苏州博瑞凯德信息技术有限公司、思科系统（中国）网络技术有限公司、深圳市迅雷网络技术有限公司、深圳市网域科技技术有限公司、深圳市牛商网络股份有限公司、深圳市麦斯杰网络有限公司、深圳市捷视飞通科技股份有限公司、深圳市皓峰通讯技术有限公司、深圳市博思协创网络科技有限公司、深圳警翼智能科技股份有限公司、深圳鼎信通达股份有限公司、上海卓卓网络科技有限公司、上海新网程信息技术股份有限公司、上海铭旭科技有限公司、上海泛微网络科技股份有限公司、青岛叁度信息技术有限公司、南宁旭东网络科技有限公司、金富瑞（北京）科技有限公司、江苏易索电子科技股份有限公司、极狐信息技术（湖北）有限公司、湖南翱云网络科技有限公司、湖北亿咖通科技有限公司、恒玄科技（上海）股份有限公司、合肥一浪网络科技有限公司、合肥海拔网络科技有限公司、杭州易软共创网络科技有限公司、哈尔滨伟成科技有限公司、广州中望龙腾软件股份有限公司、广州正脉教育技术有限公司、广州阿里巴巴文学信息技术有限公司、富士施乐（中国）有限公司、成都万江港利科技股份有限公司、畅捷通信息技术股份有限公司、北京中成科信科技发展有限公司、北京致远互联软件股份有限公司、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、北京我知科技有限公司、北京数科网维技术有限责任公司、北京时空智友科技有限公司、北京九思协同软件有限公司、北京金和网络股份有限公司、北京和信创天科技股份有限公司、北京禾唐科技有限公司、安徽省科大奥锐科技有限公司、《中国学术期刊（光盘版）》电子杂志社有限公司、台达集团、中环 CMS、若依、梦想 CM、XnSoft、Sincell, LLC、Sapido Technology Inc、MacCMS、Kalvin 在线工具、jpress、Geoserver 和 Apache Software Foundation。

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、哈尔滨安天科技集团股份有限公司、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。山东泽鹿安全技术有限公司、北京华顺信安科技有限公司、重庆都会信息科技有限公司、北京山石网科信息技术有限公司、南京众智维信息科技有限公司、内蒙古洞明科技有限公司、南京树安信息技术有限公司、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、广州百蕴启辰科技有限公司、贵州多彩宝互联网服务有限公司、北京惠而特科技有限公司、星云博创科技有限公司、河南信安世纪科技有限公司、福建省海峡信息技术有限公司、京东云安全、思而听网络科技有限公司、山东云天安全技术有限公司、广西等保安全测评有限公司、天津偕行科技有限公司、山石网科通信技术股份有限公司、杭州海康威视数字技术股份有限公司、博智安全科技股份有限公司、北京快手科技有限公司、杭州美创科技有限公司、四川哨兵信息科技有限公司、快页信息技术有限公司及其他个人白帽子向 CNVD 提交了 3412 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）、向 CNVD 共享的白帽子报送的 1459 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）	1459	1459
北京天融信网络安全技术有限公司	281	36
杭州安恒信息技术股份有限公司	206	18
哈尔滨安天科技集团股份有限公司	187	0
新华三技术有限公司	152	0
恒安嘉新（北京）科技股份公司	114	0
北京神州绿盟科技有限公司	84	15
天津市国瑞数码安全系统股份有限公司	59	0
北京启明星辰信息安全技术有限公司	59	2
北京数字观星科技有限公司	41	0
中国电信集团系统集成有限责任公司	30	0

西安四叶草信息技术有限公司	26	26
深信服科技股份有限公司	24	1
阿里云计算有限公司	10	0
北京知道创宇信息技术有限公司	5	3
北京智游网安科技有限公司	1	1
深圳市腾讯计算机系统有限公司（玄武实验室）	1	1
山东泽鹿安全技术有限公司	217	217
北京华顺信安科技有限公司	162	1
重庆都会信息科技有限公司	125	125
北京山石网科信息技术有限公司	84	84
南京众智维信息科技有限公司	43	43
内蒙古洞明科技有限公司	35	35
南京树安信息技术有限公司	31	31
河南灵创电子科技有限公司	28	28
广东蓝爵网络安全技术股份有限公司	12	12
广州百蕴启辰科技有限公司	12	12
杭州迪普科技股份有限公司	12	0
贵州多彩宝互联网服	10	10

务有限公司		
北京惠而特科技有限公司	10	10
星云博创科技有限公司	9	9
河南信安世纪科技有限公司	8	8
福建省海峡信息技术有限公司	8	8
京东云安全	8	8
亚信科技（成都）有限公司	7	0
思而听网络科技有限公司	7	7
山东云天安全技术有限公司	4	4
广西等保安全测评有限公司	4	4
天津偕行科技有限公司	3	3
山石网科通信技术股份有限公司	3	3
杭州海康威视数字技术股份有限公司	3	3
博智安全科技股份有限公司	2	2
北京快手科技有限公司	1	1
杭州美创科技有限公司	1	1
四川哨兵信息科技有限公司	1	1
快页信息技术有限公司	1	1
CNCERT 浙江分中心	1	1

个人	1178	1178
报送总计	4769	3412

本周漏洞按类型和厂商统计

本周，CNVD 收录了 353 个漏洞。WEB 应用 138 个，应用程序 118 个，网络设备（交换机、路由器等网络端设备）50 个，操作系统 19 个，智能设备（物联网终端设备）19 个，安全产品 9 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	138
应用程序	118
网络设备（交换机、路由器等网络端设备）	50
操作系统	19
智能设备（物联网终端设备）	19
安全产品	9

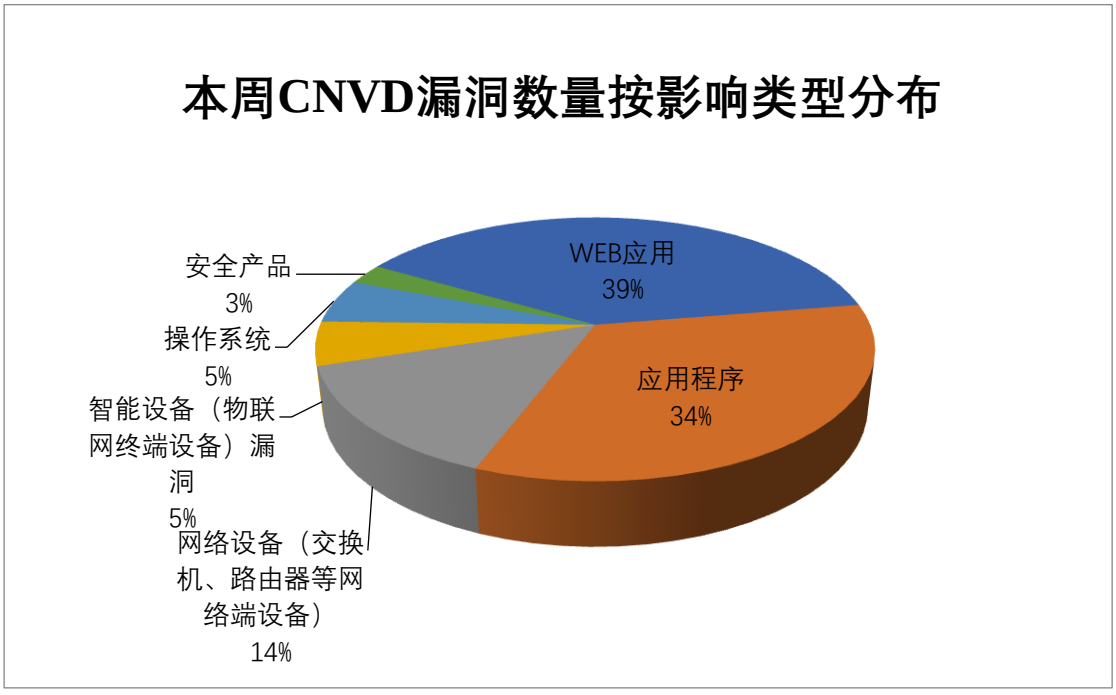

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Lantronix、Open Design Alliance、Adobe 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	Lantronix	14	4%

2	Open Design Alliance	11	3%
3	Adobe	11	3%
4	北京数科网维技术有限责任公司	11	3%
5	Garrett	9	3%
6	Apache	9	3%
7	Mozilla	9	3%
8	兄弟（中国）商业有限公司	8	2%
9	Projectworlds	8	2%
10	其他	263	74 %

本周行业漏洞收录情况

本周，CNVD 收录了 24 个电信行业漏洞，23 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，“ZyXEL GS1900 访问控制错误漏洞、Google Android Kernel 权限提升漏洞（CNVD-2022-01773）”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/

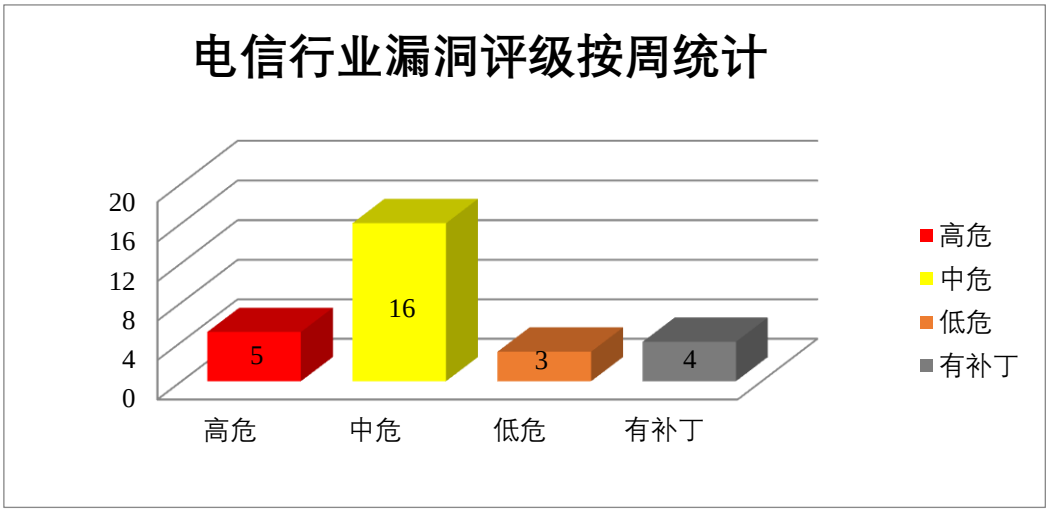

图 3 电信行业漏洞统计

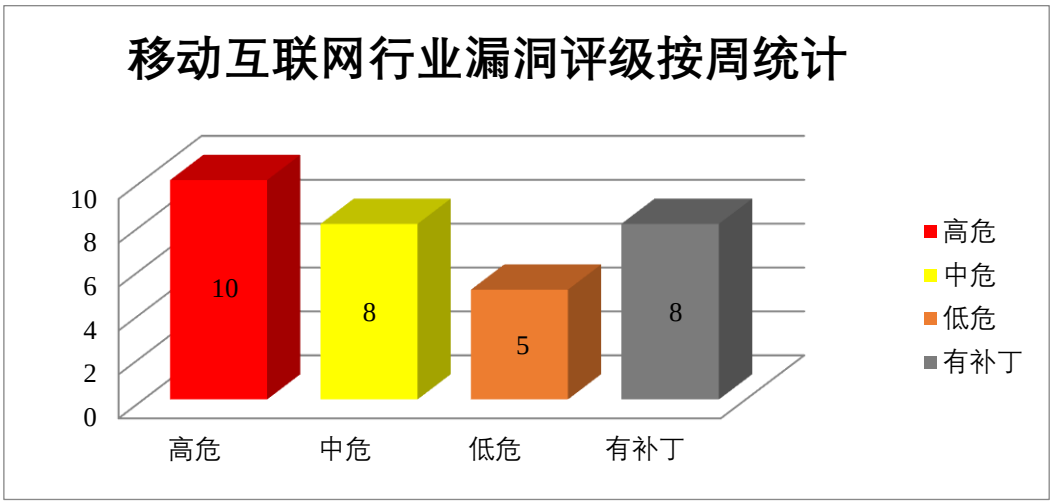

图 4 移动互联网行业漏洞统计

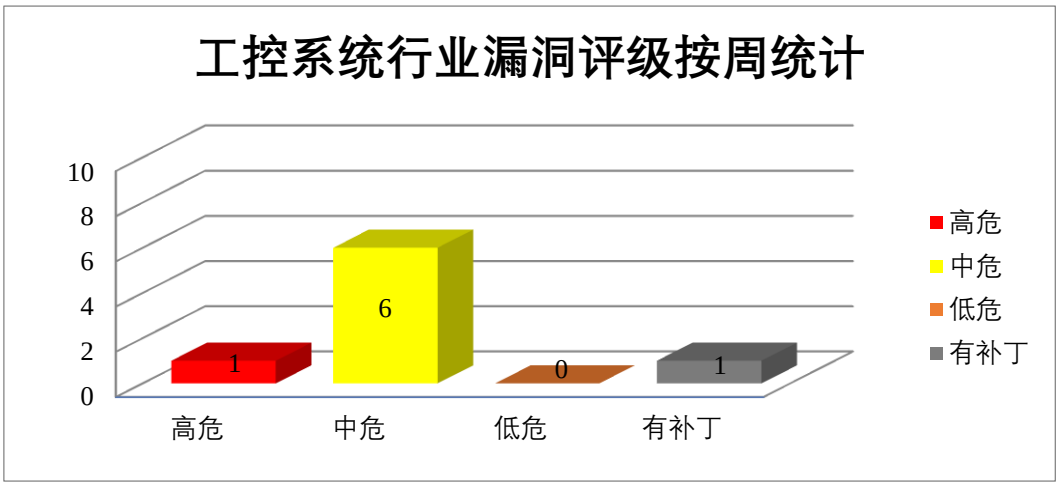

图 5 工控系统行业漏洞统计

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、 Apache 产品安全漏洞

Apache James 是美国阿帕奇（Apache）基金会的一个完全用 Java 编写的开源 Smtp 和 Pop3 邮件传输代理和 Nntp 新闻服务器。Apache Parquet 是一种列式存储格式。可用于 Hadoop 生态系统中的任何项目。Apache Log4j 是一款基于 Java 的开源日志记录工具。Apache DB DdlUtils 是美国阿帕奇（Apache）基金会的一个易于使用的小型组件，用于处理数据库定义 (DDL) 文件。Apache Storm 是一个免费开源的分布式实时计算系统。本周，上述产品被披露存在多个漏洞，攻击者可利用该漏洞造成拒绝服务攻击，远程代码执行等。

CNVD 收录的相关漏洞包括：Apache James 命令注入漏洞、Apache James 拒绝服务漏洞、Apache James 路径遍历漏洞、Apache Parquet 输入验证错误漏洞、Apache Log4j 代码执行漏洞、Apache DB DdlUtils 代码问题漏洞、Apache Storm 代码问题漏洞、

Apache log4j2 拒绝服务漏洞。其中，“Apache DB DdlUtils 代码问题漏洞、Apache Storm 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-2022-01767
https://www.cnvd.org.cn/flaw/show/CNVD-2022-01769
https://www.cnvd.org.cn/flaw/show/CNVD-2022-01768
https://www.cnvd.org.cn/flaw/show/CNVD-2022-01774
https://www.cnvd.org.cn/flaw/show/CNVD-2022-01775
https://www.cnvd.org.cn/flaw/show/CNVD-2022-01778
https://www.cnvd.org.cn/flaw/show/CNVD-2022-01777
https://www.cnvd.org.cn/flaw/show/CNVD-2022-01776

2、Lantronix 产品安全漏洞

Lantronix PremierWave 2050 是美国 Lantronix 公司的一个嵌入式企业 Wi-Fi 模块。用于提供可靠且始终在线的 5G Wi-Fi 连接。本周，上述产品被披露存在多个漏洞，攻击者可利用该漏洞导致命令执行，任意文件覆盖等。

CNVD 收录的相关漏洞包括：Lantronix PremierWave 2050 OS 命令注入漏洞（CNVD-2022-01593、CNVD-2022-01602、CNVD-2022-01599）、Lantronix PremierWave 2050 路径遍历漏洞（CNVD-2022-01594）、Lantronix PremierWave 2050 堆栈缓冲区溢出漏洞（CNVD-2022-01605、CNVD-2022-01608、CNVD-2022-01604、CNVD-2022-01607）。其中，“Lantronix PremierWave 2050 OS 命令注入漏洞（CNVD-2022-01593、CNVD-2022-01602、CNVD-2022-01599）、Lantronix PremierWave 2050 路径遍历漏洞（CNVD-2022-01594）”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-2022-01608
https://www.cnvd.org.cn/flaw/show/CNVD-2022-01607
https://www.cnvd.org.cn/flaw/show/CNVD-2022-01593
https://www.cnvd.org.cn/flaw/show/CNVD-2022-01594
https://www.cnvd.org.cn/flaw/show/CNVD-2022-01599
https://www.cnvd.org.cn/flaw/show/CNVD-2022-01602
https://www.cnvd.org.cn/flaw/show/CNVD-2022-01605
https://www.cnvd.org.cn/flaw/show/CNVD-2022-01604

3、Adobe 产品安全漏洞

Adobe Audition 是一款音频编辑器和后期制作套件。本周，上述产品被披露存在多个漏洞，攻击者可利用该漏洞导致内存泄露，执行任意代码。

CNVD 收录的相关漏洞包括：Adobe Audition 越界读取漏洞（CNVD-2022-00586、

CNVD-2022-00587）、Adobe Audition 任意代码执行漏洞（CNVD-2022-00590、CNVD-2022-00592、CNVD-2022-00591、CNVD-2022-00596、CNVD-2022-00595、CNVD-2022-00594）。其中，除“Adobe Audition 越界读取漏洞（CNVD-2022-00586、CNVD-2022-00587）”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-2022-00590
https://www.cnvd.org.cn/flaw/show/CNVD-2022-00592
https://www.cnvd.org.cn/flaw/show/CNVD-2022-00591
https://www.cnvd.org.cn/flaw/show/CNVD-2022-00596
https://www.cnvd.org.cn/flaw/show/CNVD-2022-00595
https://www.cnvd.org.cn/flaw/show/CNVD-2022-00594
https://www.cnvd.org.cn/flaw/show/CNVD-2022-00586
https://www.cnvd.org.cn/flaw/show/CNVD-2022-00587

4、Mozilla 产品安全漏洞

Mozilla Rust rusqlite crate 是一个符合人体工程学的包装器，用于使用来自 Rust 的 SQLite。它试图暴露一个类似于 rust-postgres 的接口。Mozilla Rust lru crate 是 LRU 缓存的实现。Rust libpulse-binding crate 是该存储库包含用于从 Rust 编程语言连接到 PulseAudio (PA) 的 sys (FFI) 和绑定库 (crates)。Rust actix-web crate 是一个 Rust 网络框架。Rust 是 Mozilla 基金会的一款通用、编译型编程语言。本周，上述产品被披露存在多个漏洞，攻击者可利用该漏洞造成内存破坏和拒绝服务。

CNVD 收录的相关漏洞包括：Mozilla Rust rusqlite crate 内存破坏漏洞、Mozilla Rust lru crate 释放后重用漏洞、Mozilla Rust libpulse-binding crate 内存破坏漏洞、Mozilla Rust actix-web crate 内存破坏漏洞（CNVD-2022-01146、CNVD-2022-01148、CNVD-2022-01150）、Mozilla Rust 内存破坏漏洞（CNVD-2022-01149、CNVD-2022-01151）。其中，“Mozilla Rust actix-web crate 内存破坏漏洞（CNVD-2022-01146、CNVD-2022-01148、CNVD-2022-01150）”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-2022-01143
https://www.cnvd.org.cn/flaw/show/CNVD-2022-01144
https://www.cnvd.org.cn/flaw/show/CNVD-2022-01147
https://www.cnvd.org.cn/flaw/show/CNVD-2022-01146
https://www.cnvd.org.cn/flaw/show/CNVD-2022-01148
https://www.cnvd.org.cn/flaw/show/CNVD-2022-01150
https://www.cnvd.org.cn/flaw/show/CNVD-2022-01149
https://www.cnvd.org.cn/flaw/show/CNVD-2022-01151

5、Tripexpress 路径遍历漏洞

Tripexpress 是奥地利 Shpetim Islami 个人开发者的一个开源巴士旅游旅游预订管理网络应用程序。本周，Tripexpress 被披露存在路径遍历漏洞。攻击者可利用该漏洞导致路径操作。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-2022-00625

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-2022-00616	WordPress Contest Gallery 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/45ee86a7-1497-4c81-98b8-9a8e5b3d4fac
CNVD-2022-00626	Eufy Anker Eufy Homebase 2 越界写入漏洞	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-2021-1378
CNVD-2022-00624	Made vesta 文件包含漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/myvesta/vesta/commit/88596a8cd9a9bb053d2d5bebf80c870dff49b639
CNVD-2022-00627	Eufy Anker Eufy Homebase 2 访问控制错误漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.anker.com/
CNVD-2022-01313	Garrett Metal Detectors 缓冲区溢出漏洞（CNVD-2022-01313）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://garrett.com/security/walk-through/accessories
CNVD-2022-01319	Garrett Metal Detectors 路径遍历漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://garrett.com/security/walk-through/accessories
CNVD-2022-01326	Projectworlds House Rental 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://projectworlds.in/
CNVD-2022	Huawei HarmonyOS 输入验	高	目前厂商已发布升级补丁以修复漏

-01676	证错误漏洞（CNVD-2022-01676）		洞，详情请关注厂商主页：https://device.harmonyos.com/cn/docs/security/update/security-bulletins-202109-0000001196270727
CNVD-2022-01682	Zyxel NBG6604 访问控制错误漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://www.zyxel.com/support/Zyxel_security_advisory_for_sensitive_information_vulnerabilities_of_NBG6604_home_router.shtml
CNVD-2022-01686	Microsoft SharePoint 权限提升漏洞（CNVD-2022-01686）	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://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-43876

小结：本周，Apache 产品被披露存在多个漏洞，攻击者可利用该漏洞造成拒绝服务攻击，远程代码执行等。此外，Lantronix、Adobe、Mozilla 等多款产品被披露存在多个漏洞，攻击者可利用该漏洞造成内存破坏，拒绝服务，执行任意代码，任意文件覆盖等。另外，Tripexpress 被披露存在路径遍历漏洞。攻击者可利用该漏洞导致路径操作。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、projectworlds car rental management system 跨站脚本漏洞

验证描述

projectworlds car rental management system 是 projectworlds 的一个汽车租赁管理系统。

projectworlds car rental management system 存在跨站脚本漏洞，攻击者可利用该漏洞获取一个管理登录会话 cookie，并在一个管理登录时窃取一个管理会话。

验证信息

POC 链接：https://packetstormsecurity.com/files/158795/Car-Rental-Management-System-1.0-Cross-Site-Scripting.html

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2022-01325

信息提供者

哈尔滨安天科技集团股份有限公司

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 解决 Workstation、Fusion 和 ESXi 产品中堆溢出漏洞

VMware 发布了安全更新，以解决其 Workstation、Fusion 和 ESXi 产品中的堆溢出漏洞（编号为 CVE-2021-22045）。该问题可能导致在虚拟机管理程序上执行代码。

参考链接：https://securityaffairs.co/wordpress/126352/security/vmware-cve-2021-22045-heap-overflow.html

2. 苹果 iOS 曝 doorLock 漏洞，能让手机“变砖”

苹果 Apple HomeKit 中发现了一个名为“doorLock”的新型持续拒绝服务漏洞，影响的系统版本从 IOS14.7 到 IOS15.2。

参考链接：https://www.freebuf.com/articles/318193.html

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