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 21 日-2022 年 02 月 27 日 **2022 年第 8 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 429 个，其中高危漏洞 152 个、中危漏洞 243 个、低危漏洞 34 个。漏洞平均分值为 6.09。本周收录的漏洞中，涉及 0day 漏洞 209 个（占 49%），其中互联网上出现“jonfinley Monitorr 授权绕过漏洞、Npm ps-kill 命令注入漏洞”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 5012 个，与上周（4976 个）环比增加 0.7%。

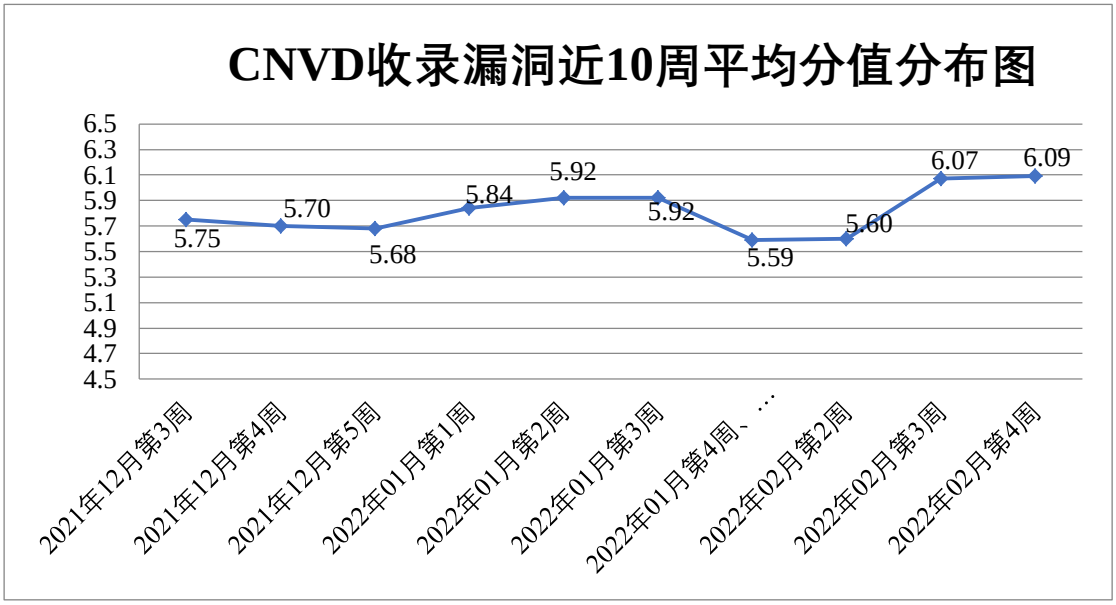

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 35 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 713 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 54 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 72 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：

珠海新华通软件股份有限公司、重庆中联信息产业有限责任公司、重庆泛普软件有限公司、中山市同创科技发展有限公司、智互联（深圳）科技有限公司、郑州维维信息技术有限公司、正方软件股份有限公司、浙江大华技术股份有限公司、浙江阿拉丁信息科技股份有限公司、长城广联（北京）国际广告有限公司、圆梦云科技有限公司、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、西门子（中国）有限公司、西安微光软件科技有限公司、西安网卓信息技术有限公司、西安交大捷普网络科技有限公司、武汉深之度科技有限公司、武汉富思特创新信息技术有限公司、无锡城安信息科技有限公司、温州市易天信息科技有限公司、微软（中国）有限公司、索尼（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、深圳市迅雷网络技术有限公司、深圳市迅捷通信技术有限公司、深圳市乔安科技有限公司、深圳市磊科实业有限公司、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、深圳勤杰软件有限公司、深圳齐心好视通云计算有限公司、深圳警翼智能科技股份有限公司、深圳华磊物流通信息科技有限公司、上海云翌通信科技有限公司、上海荃路软件开发工作室、上海汉得信息技术股份有限公司、上海泛微软件有限公司、上海二三四五网络科技有限公司、上海贝锐信息科技股份有限公司、上海艾泰科技有限公司、山东思达特测控设备有限公司、山东力创科技股份有限公司、山东捷瑞数字科技股份有限公司、厦门四信通信科技有限公司、任子行网络技术股份有限公司、全讯汇聚网络科技（北京）有限公司、普联技术有限公司、欧姆龙自动化（中国）有限公司、牛迈网络科技有限公司、南宁旭东网络科技有限公司、南昌腾速科技有限公司、廊坊市极致网络科技有限公司、蓝网科技股份有限公司、吉翁电子（深圳）有限公司、华硕电脑（上海）有限公司、河北南昊高新技术开发有限公司、合肥翰林数码科技有限公司、航天信息股份有限公司、杭州吉拉科技有限公司、杭州海康威视数字技术股份有限公司、杭州晨科软件技术有限公司、国泰新点软件股份有限公司、广州同鑫科技有限公司、广州市颖峰信息科技有限公司、福州网钛软件科技有限公司、福建科立讯通信有限公司、德国 3S 软件有限公司、成都万江港利科技有限公司、成都康特电子科技股份有限公司、北京印象笔记科技有限公司、北京星网锐捷网络技术有限公司、北京万户网络技术有限公司、北京天星组态软件有限公司、北京神州视翰科技有限公司、北京仁和汇智信息技术有限公司、北京清元优软科技有限公司、北京勤云科技发展有限公司、北京派网软件有限公司、北京慕华信息科技有限公司、北京猎鹰安全科技有限公司、北京九思协同软件有限公司、北京国通创安报警网络技术有限公司、北京高速波软件有限公司、北京东华

原医疗设备有限责任公司、北京东方通科技股份有限公司、北京北大方正电子有限公司、北京百卓网络技术有限公司、安徽省科大奥锐科技有限公司、中新金盾、台达集团、京瓷集团、勾股 CMS、北京和利时集团、zzzcms、ZZCMS、Yamaha Corporation、TOTOLINK、The Apache Software Foundation、Rockwell Automation、PhpaaCMS、Oracle、NGINX, Inc.、NETGEAR、INTELLINET、F5、Emerson、DEVA Broadcast Ltd.、Conextop Technologies Co、CatfishCMS 和 Arista Networks。

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，北京启明星辰信息安全技术有限公司、杭州安恒信息技术股份有限公司、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等单位报送公开收集的漏洞数量较多。山东云天安全技术有限公司、北京山石网科信息技术有限公司、长春嘉诚信息技术股份有限公司、山东新潮信息技术有限公司、开元华创科技集团、上海纽盾科技股份有限公司、内蒙古洞明科技有限公司、南京树安信息技术有限公司、北京安华金和科技有限公司、杭州默安科技有限公司、广州百蕴启辰科技有限公司、河南信安世纪科技有限公司、河南东方云盾信息技术有限公司、山石网科通信技术股份有限公司、广东蓝爵网络安全技术股份有限公司、华鲁数智信息技术（北京）有限公司、南京禾盾信息科技有限公司、贵州多彩宝互联网服务有限公司、重庆都会信息科技有限公司、江苏保旺达软件技术有限公司、山东泽鹿安全技术有限公司、北京远禾科技有限公司、海南神州希望网路有限公司、河南灵创电子科技有限公司、天津偕行科技有限公司、博智安全科技股份有限公司、有度网络安全技术有限公司、苏州棱镜七彩信息科技有限公司、成都智安民扬网络有限公司、贵州泰若数字科技有限公司、北京威努特技术有限公司、武汉安域信息安全技术有限公司、深圳昂楷科技有限公司、新疆安疆科技有限公司、快页信息技术有限公司、广东物壹信息科技股份有限公司及其他个人白帽子向 CNVD 提交了 5012 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 2161 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）	1310	1310
上海交大	462	462
奇安信网神（补天平台）	389	389
北京启明星辰信息安全技术有限公司	289	233

杭州安恒信息技术股份有限公司	255	97
新华三技术有限公司	234	0
安天科技集团股份有限公司	215	0
北京天融信网络安全技术有限公司	145	45
恒安嘉新（北京）科技股份公司	123	0
北京神州绿盟科技有限公司	119	10
北京数字观星科技有限公司	91	0
南京众智维信息科技有限公司	61	61
天津市国瑞数码安全系统股份有限公司	59	0
深信服科技股份有限公司	47	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	29	29
北京安信天行科技有限公司	14	14
卫士通信息产业股份有限公司	2	2
北京长亭科技有限公司	1	1
北京华顺信安科技有限公司	122	0
山东云天安全技术有限公司	63	63
亚信科技（成都）有限公司	62	0

北京山石网科信息技术有限公司	60	60
长春嘉诚信息技术股份有限公司	59	59
山东新潮信息技术有限公司	30	30
西门子（中国）有限公司	25	0
开元华创科技集团	19	19
上海纽盾科技股份有限公司	14	14
内蒙古洞明科技有限公司	14	14
南京树安信息技术有限公司	14	14
北京安华金和科技有限公司	14	14
杭州迪普科技股份有限公司	14	0
杭州默安科技有限公司	13	13
广州百蕴启辰科技有限公司	13	13
河南信安世纪科技有限公司	10	10
河南东方云盾信息技术有限公司	8	8
山石网科通信技术股份有限公司	7	7
广东蓝爵网络安全技术股份有限公司	7	7
华鲁数智信息技术（北京）有限公司	5	5
南京禾盾信息科技有限公司	5	5

贵州多彩宝互联网服务有限公司	5	5
重庆都会信息科技有限公司	5	5
江苏保旺达软件技术有限公司	3	3
山东泽鹿安全技术有限公司	2	2
北京远禾科技有限公司	2	2
海南神州希望网路有限公司	2	2
河南灵创电子科技有限公司	2	2
天津偕行科技有限公司	2	2
博智安全科技股份有限公司	1	1
有度网络安全技术有限公司	1	1
苏州棱镜七彩信息科技有限公司	1	1
成都智安民扬网络有限公司	1	1
贵州泰若数字科技有限公司	1	1
北京威努特技术有限公司	1	1
武汉安域信息安全技术有限公司	1	1
深圳昂楷科技有限公司	1	1
新疆安疆科技有限公司	1	1
快页信息技术有限公	1	1

司		
广东物壹信息科技股份有限公司	1	1
CNCERT 山西分中心	5	5
CNCERT 四川分中心	1	1
个人	1964	1964
报送总计	6457	5012

本周漏洞按类型和厂商统计

本周，CNVD 收录了 429 个漏洞。WEB 应用 139 个，应用程序 138 个，网络设备（交换机、路由器等网络端设备）73 个，智能设备（物联网终端设备）28 个，操作系统 26 个，数据库 17 个，安全产品 8 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	139
应用程序	138
网络设备（交换机、路由器等网络端设备）	73
智能设备（物联网终端设备）	28
操作系统	26
数据库	17
安全产品	8

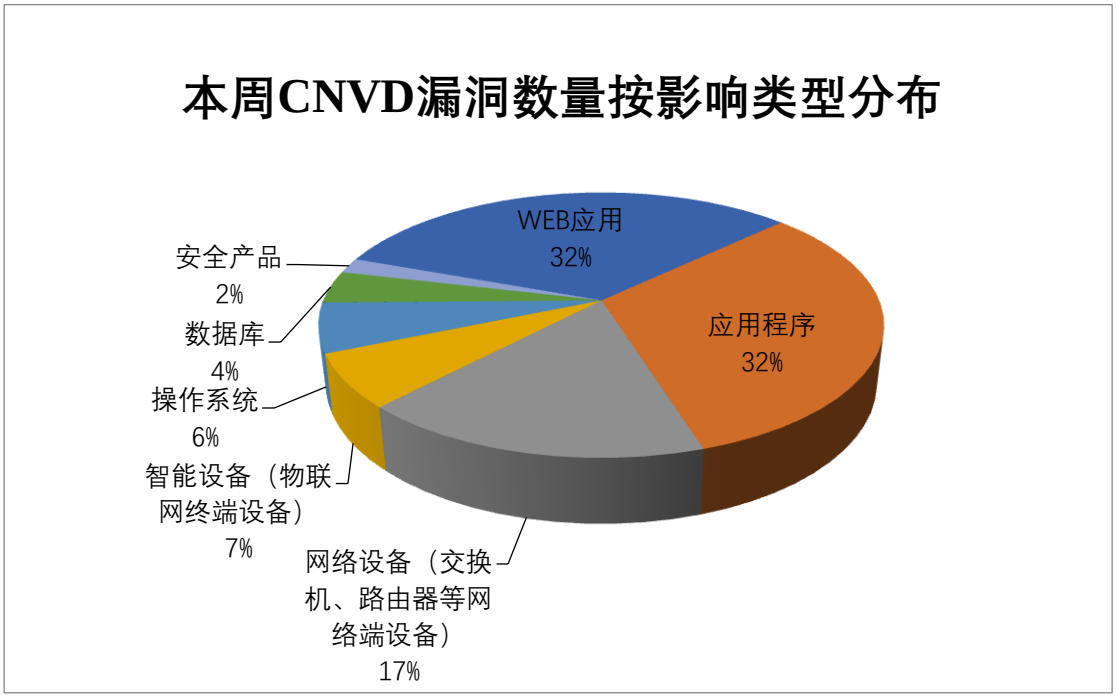

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Google、Tenda、Huawei 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	Google	40	9%
2	Tenda	16	4%
3	Huawei	15	3%
4	北京棣南新宇科技有限公司	14	3%
5	XWiki	14	3%
6	Oracle	14	3%
7	广州添富信息科技有限公司	13	3%
8	Apache	12	3%
9	Reolink	11	3%
10	其他	280	66%

本周行业漏洞收录情况

本周，CNVD 收录了 50 个电信行业漏洞，11 个移动互联网行业漏洞，20 个工控行业漏洞（如下图所示）。其中，“Tenda AC Series Router 缓冲区溢出漏洞、Huawei E mui 越界访问漏洞”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/

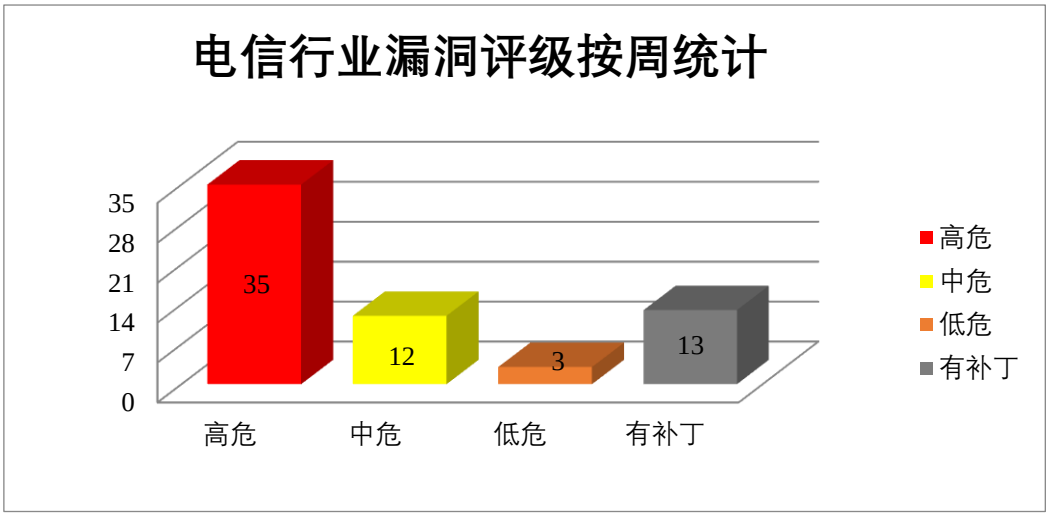

图 3 电信行业漏洞统计

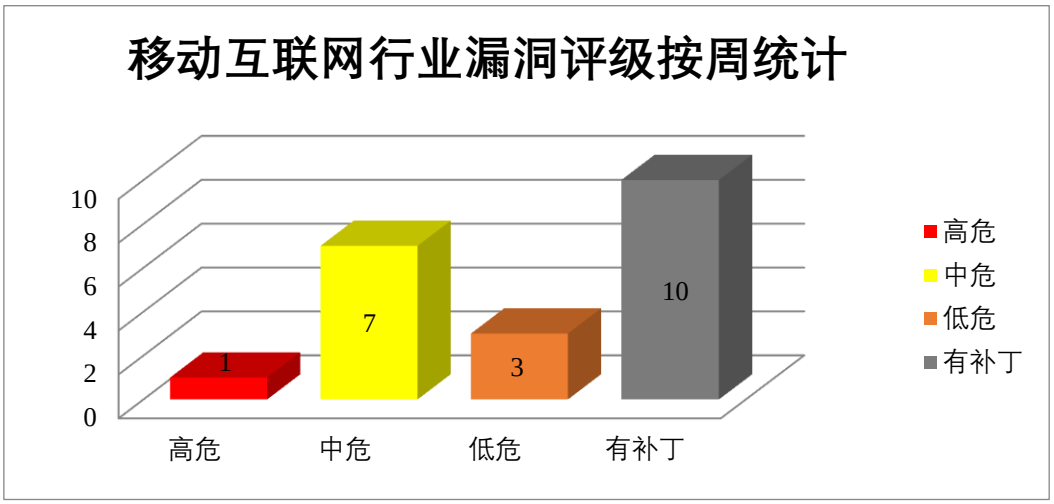

图 4 移动互联网行业漏洞统计

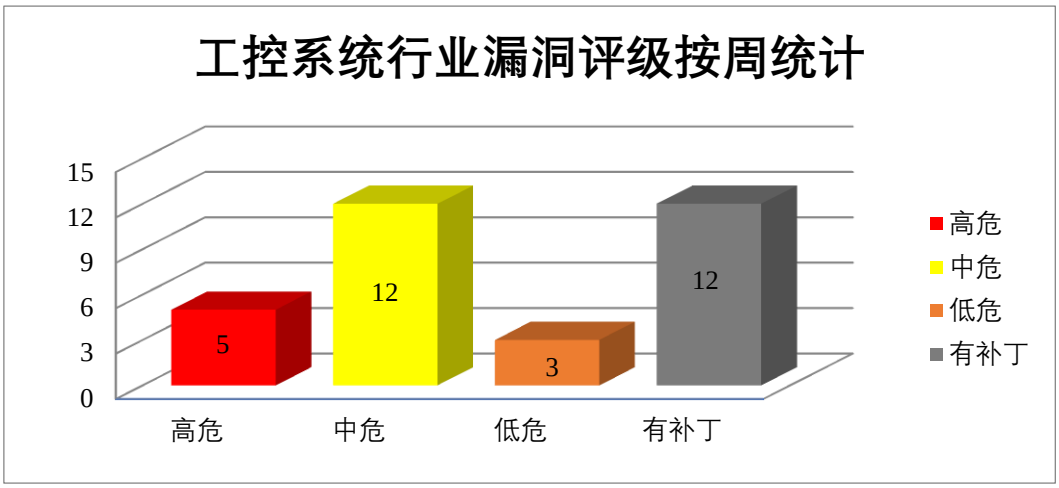

图 5 工控系统行业漏洞统计

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、 Google 产品安全漏洞

Google Chrome 是美国谷歌（Google）公司的一款 Web 浏览器。本周，上述产品被披露存在资源管理错误漏洞，攻击者可利用漏洞通过精心设计的 HTML 页面利用堆损坏，在目标系统上执行任意代码等。

CNVD 收录的相关漏洞包括：Google Chrome 资源管理错误漏洞（CNVD-2022-14876、CNVD-2022-15136、CNVD-2022-15137、CNVD-2022-15140、CNVD-2022-15142、CNVD-2022-15157、CNVD-2022-15160、CNVD-2022-15159）。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-2022-14876

https://www.cnvd.org.cn/flaw/show/CNVD-2022-15136

https://www.cnvd.org.cn/flaw/show/CNVD-2022-15137

https://www.cnvd.org.cn/flaw/show/CNVD-2022-15140

https://www.cnvd.org.cn/flaw/show/CNVD-2022-15142

https://www.cnvd.org.cn/flaw/show/CNVD-2022-15157

https://www.cnvd.org.cn/flaw/show/CNVD-2022-15160

https://www.cnvd.org.cn/flaw/show/CNVD-2022-15159

2、 Apache 产品安全漏洞

Apache Apisix 是美国阿帕奇（Apache）基金会的一个云原生的微服务 API 网关服务。Apache HTTP Server 是一款开源网页服务器。Apache ActiveMQ 是一套开源的消息中间件，它支持 Java 消息服务、集群、Spring Framework 等。Apache Cayenne 是一个根据 Apache 许可证许可的开源持久性框架。Apache Pulsar 是一个用于云环境种，集消息、存储、轻量化函数式计算为一体的分布式消息流平台。Apache Cassandra 是一个分布式 Nosql 数据库。Xerces 是一个由 Apache 组织所推动的一项 XML 文档解析开源项目。Apache Kafka 是一套开源分布式流媒体平台。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞获取访问凭据并提升系统权限，执行拒绝服务(DoS)攻击，在主机上执行任意代码等。

CNVD 收录的相关漏洞包括：Apache Apisix 远程代码执行漏洞、Apache HTTP Server 代码问题漏洞（CNVD-2022-13199）、Apache ActiveMQ 资源管理错误漏洞（CNVD-2022-14699）、Apache Cayenne 输入验证错误漏洞、Apache Pulsar 输入验证错误漏洞、Apache Cassandra 代码注入漏洞、Apache Xerces 拒绝服务漏洞、Apache Kafka 定时攻击漏洞。其中“Apache Apisix 远程代码执行漏洞、Apache Cassandra 代码注入漏洞、Apache Xerces 拒绝服务漏洞、Apache Kafka 定时攻击漏洞”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-2022-12799

https://www.cnvd.org.cn/flaw/show/CNVD-2022-13199

https://www.cnvd.org.cn/flaw/show/CNVD-2022-14699

https://www.cnvd.org.cn/flaw/show/CNVD-2022-14702

https://www.cnvd.org.cn/flaw/show/CNVD-2022-14705

https://www.cnvd.org.cn/flaw/show/CNVD-2022-14703

https://www.cnvd.org.cn/flaw/show/CNVD-2022-14709

https://www.cnvd.org.cn/flaw/show/CNVD-2022-14712

3、 Oracle 产品安全漏洞

Oracle MySQL 是美国甲骨文（Oracle）公司的一套开源的关系数据库管理系统。M

ySQL Cluster 是其中的一个适用于分布式计算环境的高实用、高冗余的版本。本周，上述产品被披露存在输入验证错误漏洞，攻击者可利用漏洞读取内存内容或使应用程序崩溃，执行任意代码等。

CNVD 收录的相关漏洞包括：Oracle MySQL Cluster 输入验证错误漏洞（CNVD-2022-13051、CNVD-2022-13054、CNVD-2022-13052、CNVD-2022-13056、CNVD-2022-13055、CNVD-2022-13058、CNVD-2022-13062、CNVD-2022-13061）。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-2022-13051
https://www.cnvd.org.cn/flaw/show/CNVD-2022-13054
https://www.cnvd.org.cn/flaw/show/CNVD-2022-13052
https://www.cnvd.org.cn/flaw/show/CNVD-2022-13056
https://www.cnvd.org.cn/flaw/show/CNVD-2022-13055
https://www.cnvd.org.cn/flaw/show/CNVD-2022-13058
https://www.cnvd.org.cn/flaw/show/CNVD-2022-13062
https://www.cnvd.org.cn/flaw/show/CNVD-2022-13061

4、Schneider Electric 产品安全漏洞

Schneider Electric Interactive Graphical SCADA System（IGSS）是法国施耐德电气（Schneider Electric）公司的一套用于监控和控制工业过程的 SCADA（数据采集与监控系统）系统。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞删除任意文件，导致远程代码执行等。

CNVD 收录的相关漏洞包括：Schneider Electric Interactive Graphical SCADA System 访问控制错误漏洞（CNVD-2022-13067、CNVD-2022-13073）、Schneider Electric Interactive Graphical Scada System 整数溢出漏洞、Schneider Electric Interactive Graphical SCADA System 缓冲区溢出漏洞（CNVD-2022-13069、CNVD-2022-13075）、Schneider Electric Interactive Graphical SCADA System 路径遍历漏洞（CNVD-2022-13068）、Schneider Electric Interactive Graphical Scada System 越界读取漏洞（CNVD-2022-13070、CNVD-2022-13071）。其中“Schneider Electric Interactive Graphical Scada System 整数溢出漏洞、Schneider Electric Interactive Graphical SCADA System 缓冲区溢出漏洞（CNVD-2022-13069、CNVD-2022-13075）、Schneider Electric Interactive Graphical SCADA System 路径遍历漏洞（CNVD-2022-13068）”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-2022-13067
https://www.cnvd.org.cn/flaw/show/CNVD-2022-13066

https://www.cnvd.org.cn/flaw/show/CNVD-2022-13069

https://www.cnvd.org.cn/flaw/show/CNVD-2022-13068

https://www.cnvd.org.cn/flaw/show/CNVD-2022-13071

https://www.cnvd.org.cn/flaw/show/CNVD-2022-13070

https://www.cnvd.org.cn/flaw/show/CNVD-2022-13073

https://www.cnvd.org.cn/flaw/show/CNVD-2022-13075

5、Tenda Ax3 缓冲区溢出漏洞（CNVD-2022-13931）

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列表参数造成拒绝服务 (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-2022-13931

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-2022-12807	Siemens Simcenter Femap 缓冲区溢出漏洞	高	厂商已发布相关补丁，请及时更新：https://new.siemens.com/cn/zh.html
CNVD-2022-12818	Reolink RLC-410W TestEmail 功能越界写入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://reolink.com/us/product/rlc-410w/
CNVD-2022-13078	Sourcecodester Online Project Time Management System 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/nu11secur1ty/CVE-nu11secur1ty/tree/main/vendors/oretnom23/2022/Online-Project-Time-Management
CNVD-2022-13182	Huawei HarmonyOS 代码注入漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://device.harmonyos.com/cn/docs/security/update/security-bulletins-202110-0000001162998526
CNVD-2022-13190	FeehiCMS 代码问题漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://github.com/liufee/cms/issues/44
CNVD-2022-13189	Amazon WorkSpaces 参数注入漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

			https://docs.aws.amazon.com/workspaces/latest/userguide/amazon-workspaces-windows-client.html#windows-release-notes
CNVD-2022-13198	Gradle 操作系统命令注入漏洞	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/gradle/gradle/security/advisories/GHSA-6j2p-252f-7mw8
CNVD-2022-13197	Totolink A720R 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://github.com/hurricane618/my_cves/blob/master/router/totolink/A720R_leak_config_file.md
CNVD-2022-13205	microweber 跨站脚本漏洞（CNVD-2022-13205）	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/microweber/microweber/commit/f7f5d41ba1a08ceed37c00d5f70a3f48b272e9f2
CNVD-2022-13353	eliteCMS /admin/edit_user.php 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/jsjbcyber/bug_report/blob/main/bug_f

小结：本周，Google 产品被披露存在多个漏洞，攻击者可利用漏洞通过精心设计的 HTML 页面利用堆损坏，在目标系统上执行任意代码等。此外，Apache、Oracle、Schneider Electric 等多款产品被披露存在多个漏洞，攻击者可利用漏洞获取访问凭据并提升系统权限，删除任意文件，执行拒绝服务(DoS)攻击，在主机上执行任意代码等。另外，Tenda AX3 被披露存在缓冲区溢出漏洞。攻击者可利用漏洞通过列表参数造成拒绝服务 (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、Npm ps-kill 命令注入漏洞

验证描述

Npm ps-kill 是美国 （Npm）公司的一个应用软件。提供轻松杀死进程功能。

Npm ps-kill 存在命令注入漏洞，攻击者可利用该漏洞执行任意命令。

验证信息

POC 链接：https://security.snyk.io/vuln/SNYK-JS-PSKILL-1078529

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2022-13079

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. CISA 已知利用漏洞列表中，新增两个 Zabbix 漏洞

美国 CISA 在其已知利用漏洞目录中，添加了两个影响 Zabbix 基础设施监控工具的漏洞。

参考链接：https://securityaffairs.co/wordpress/128374/hacking/cisa-zabbix-flaws.html

2. 三星上亿部手机曝出严重加密漏洞

据估计，三星累积出货了 1 亿部存在严重加密漏洞的智能手机，包括从 2017 年的 Galaxy S8 到去年的 Galaxy S21 的各种型号。

参考链接：https://www.secrss.com/articles/39656

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