国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2022 年 04 月 18 日-2022 年 04 月 24 日 **2022 年第 16 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 369 个，其中高危漏洞 110 个、中危漏洞 219 个、低危漏洞 40 个。漏洞平均分值为 5.81。本周收录的漏洞中，涉及 0day 漏洞 192 个（占 52%），其中互联网上出现“AeroCMS 跨站脚本漏洞（CNVD-2022-30784）、CxuuCms 跨站脚本漏洞（CNVD-2022-31818）”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 9337 个，与上周（4626 个）环比增加 102%。

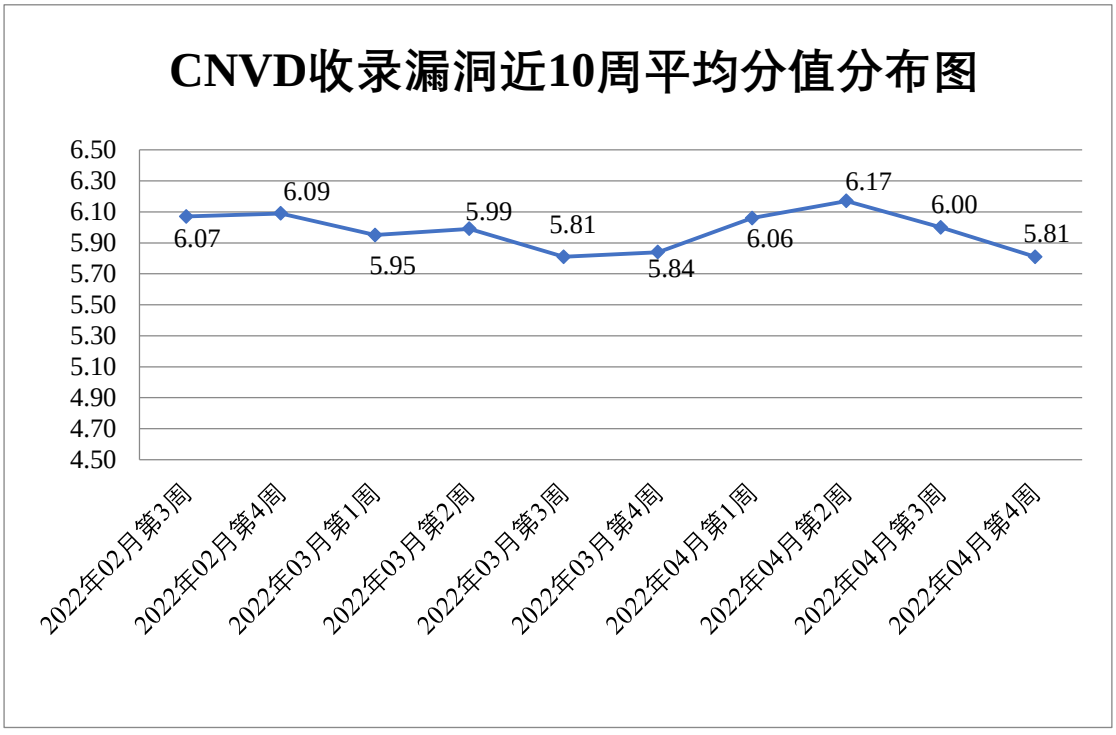

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 83 起，向基础电信企业通报漏洞事件 60 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 940 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 119 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 160 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：

紫光股份有限公司、淄博闪灵网络科技有限公司、珠海奥威软件科技有限公司、重庆中联信息产业有限责任公司、重庆楚捷科技有限公司、众勤通信设备贸易（上海）有限公司、中易云（唐山）物联网科技有限公司、中国南玻集团股份有限公司、郑州木云电子科技有限公司、浙江宇视科技有限公司、长沙米拓信息技术有限公司、云南链滴科技有限公司、昱能科技股份有限公司、用友网络科技股份有限公司、易赴科技（集团）有限公司、兄弟（中国）商业有限公司、新开普电子股份有限公司、西安九佳易信息资讯有限公司、西安建大静态交通研究院有限公司、西安佰联网络技术有限公司、武汉天地伟业科技有限公司、武汉客客信息技术有限公司、武汉渐入佳竞网络科技有限公司、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、通用电气（GE）公司、台达电子企业管理（上海）有限公司、苏州科达科技股份有限公司、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、视联动力信息技术股份有限公司、深圳云安宝科技有限公司、深圳维盟科技股份有限公司、深圳市迅捷通信技术有限公司、深圳市微客互动有限公司、深圳市网域科技技术有限公司、深圳市万网博通科技有限公司、深圳市思迅软件股份有限公司、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、上海卓佑计算机技术有限公司、上海远丰信息科技（集团）有限公司、上海盈策信息技术有限公司、上海银宇信息技术有限公司、上海携宁计算机科技股份有限公司、上海物创信息科技有限公司、上海七牛信息技术有限公司、上海纳宇电气有限公司、上海宽尔网络科技有限公司、上海肯特仪表股份有限公司、上海鸿翼软件技术股份有限公司、上海海典软件股份有限公司、上海孚盟软件有限公司、上海泛微网络科技股份有限公司、上海二三四五网络科技有限公司、上海缔安科技股份有限公司、上海大汉三通数据通信有限公司、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、山东康程信息科技有限公司、山东环球软件股份有限公司、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、三星（中国）投资有限公司、瑞昱半导体股份有限公司、融成（天津）信息技术有限公司、任子行网络股份有限公司、群晖网络科技（上海）有限公司、麒麟软件有限公司、南京云网汇联软件技术有限公司、南京酷软软件有限公司、南京笨驴信息技术有限公司、美的集团股份有限公司、满金坝（深圳）科技有限公司、临沭县俊泽商贸有限公司、朗坤智慧科技股份有限公司、廊坊市极致网络科技有限公司、

江苏曼荼罗软件股份有限公司、佳能（中国）有限公司、济南拓兴电子科技有限公司、济南亘安信息技术有限公司、吉翁电子（深圳）有限公司、惠普贸易（上海）有限公司、华硕电脑（上海）有限公司、湖南建研信息技术股份有限公司、湖南创星科技股份有限公司、湖南奥科网络技术股份有限公司、湖北点点点科技有限公司、恒热投资控股有限公司、河南新远方商翼电子科技有限公司、河南恩熙信息技术有限公司、河北利万信息科技有限公司、杭州益仕行信息技术有限公司、杭州雄伟科技开发股份有限公司、杭州图特信息科技有限公司、杭州荷花软件有限公司、杭州贝腾科技有限公司、汉王科技股份有限公司、海南赞赞网络科技有限公司、哈尔滨新中新电子股份有限公司、广州月月鸟智能科技有限公司、广州倚和视光科技有限公司、广州图创计算机软件开发有限公司、广州齐博网络科技有限公司、广州灵犀互动娱乐有限公司、广州巨杉软件开发有限公司、广州红帆科技有限公司、广联达科技股份有限公司、福州凌顶软件有限公司、东莞市天策网络科技有限公司、大唐电信科技股份有限公司、大连贝芙瑞美容服务有限公司、成都同飞科技有限责任公司、北京中创视讯科技有限公司、北京智网科技股份有限公司、北京云帆互联科技有限公司、北京星网锐捷网络技术有限公司、北京象新力科技有限公司、北京五指互联科技有限公司、北京网御星云信息技术有限公司、北京通达信科科技有限公司、北京天威诚信电子商务服务有限公司、北京神州数码云科信息技术有限公司、北京上元信安技术有限公司、北京九思协同软件有限公司、北京宏业超世纪科技有限公司、北京东华原医疗设备有限责任公司、北京超图软件股份有限公司、北京碧海威科技有限公司、北京百卓网络技术有限公司、北京百变悟空科技有限公司、安科瑞电气股份有限公司、安川电机（中国）有限公司、阿里巴巴集团安全应急响应中心、沈阳市皇姑区爱浓网络技术服务中心、梓豪团队、三菱电机株式会社、梦想 CMS、zzzcms、ZZCMS、X6CMS、VMware、Sonatype、SeaCMS、Redis、Pluck CMS、PHPGurukul、OneBlog、NETGEAR、MinIO、JreCms、Fronius、FANUC、DM 建站系统、CuppaCMS、Cesanta 和 Adobe。

本周，CNVD 发布了《Oracle 发布 2022 年 4 月的安全公告》。详情参见 CNVD 网站公告内容。

https://www.cnvd.org.cn/webinfo/show/7626

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，深信服科技股份有限公司、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、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。北京华顺信安科技有限公司、杭州海康威视数字技术股份有限公司、北京山石网科信息技术有限公司、北京云科安信科技有限公司（Seraph 安全实验室）、长春嘉诚信息技术股份有限公司、内蒙古洞明科技有限公司、

杭州迪普科技股份有限公司、南京树安信息技术有限公司、北京水木羽林科技有限公司、上海纽盾科技股份有限公司、贵州泰若数字科技有限公司、重庆都会信息科技、河南灵创电子科技有限公司、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、河北千诚电子科技有限公司、河南东方云盾信息技术有限公司、北京百度网讯科技有限公司、快页信息技术有限公司、山东云天安全技术有限公司、交通运输信息安全中心有限公司、山石网科通信技术股份有限公司、武汉安域信息安全技术有限公司、广西等保安全测评有限公司、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、河南省鼎信信息安全等级测评有限公司、北京惠而特科技有限公司、赛尔网络有限公司山东分公司、南京节点安全技术有限公司、河北华测信息技术有限公司、深圳市魔方安全科技有限公司、南京深安科技有限公司、北京威努特技术有限公司、江苏天竞云合数据技术有限公司、麒麟软件有限公司、广西塔易信息技术有限公司、上海上讯信息技术股份有限公司、南京禾盾信息科技有限公司、北京机沃科技有限公司、苏州棱镜七彩信息科技有限公司、海南神州希望网络有限公司、京东探索研究院信息安全实验室、联想集团、任子行网络技术股份有限公司及其他个人白帽子向 CNVD 提交了 9337 个以事件型漏洞为主的原创漏洞，其中包括上海交大、斗象科技（漏洞盒子）和奇安信网神（补天平台）向 CNVD 共享的白帽子报送的 5979 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
上海斗象信息科技有限公司（漏洞盒子）	3849	3849
深信服科技股份有限公司	2522	0
网神信息技术（北京）股份有限公司	1640	1640
上海交大	490	490
新华三技术有限公司	392	0
三六零数字安全科技集团有限公司	338	338
安天科技集团股份有限公司	263	0
北京天融信网络安全技术有限公司	231	37
北京神州绿盟科技	155	5

有限公司		
杭州安恒信息技术股份有限公司	150	150
北京启明星辰信息安全技术有限公司	127	22
恒安嘉新（北京）科技股份公司	100	0
北京数字观星科技有限公司	96	0
内蒙古云科数据服务股份有限公司	89	89
天津市国瑞数码安全系统股份有限公司	59	0
南京众智维信息科技有限公司	37	37
西安四叶草信息技术有限公司	28	28
中国电信集团系统集成有限责任公司	25	0
南京联成科技发展股份有限公司	20	20
北京知道创宇信息技术有限公司	11	5
京东科技信息技术有限公司	9	9
深圳市腾讯计算机系统有限公司（玄武实验室）	7	7
远江盛邦（北京）网络安全科技股份有限公司	6	6
卫士通信息产业股份有限公司	4	4
北京华顺信安科技	294	1

有限公司		
杭州海康威视数字技术股份有限公司	125	125
北京山石网科信息技术有限公司	116	116
北京云科安信科技有限公司（Seraph 安全实验室）	103	103
亚信科技（成都）有限公司	75	0
长春嘉诚信息技术股份有限公司	51	51
内蒙古洞明科技有限公司	51	51
杭州迪普科技股份有限公司	27	13
南京树安信息技术有限公司	19	19
北京水木羽林科技有限公司	14	14
上海纽盾科技股份有限公司	13	13
贵州泰若数字科技有限公司	12	12
重庆都会信息科技	10	10
河南灵创电子科技有限公司	10	10
河南信安世纪科技有限公司	10	10
福建省海峡信息技术有限公司	9	9
河北千诚电子科技有限公司	8	8
河南东方云盾信息技术有限公司	8	8

北京百度网讯科技有限公司	6	6
快页信息技术有限公司	6	6
山东云天安全技术有限公司	3	3
交通运输信息安全中心有限公司	3	3
山石网科通信技术股份有限公司	3	3
武汉安域信息安全技术有限公司	3	3
广西等保安全测评有限公司	3	3
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
河南省鼎信信息安全等级测评有限公司	2	2
北京惠而特科技有限公司	2	2
赛尔网络有限公司山东分公司	2	2
南京节点安全技术有限公司	2	2
河北华测信息技术有限公司	2	2
深圳市魔方安全科技有限公司	2	2
南京深安科技有限公司	2	2
北京威努特技术有限公司	1	1

江苏天竞云合数据技术有限公司	1	1
麒麟软件有限公司	1	1
广西塔易信息技术有限公司	1	1
上海上讯信息技术股份有限公司	1	1
南京禾盾信息科技有限公司	1	1
北京机沃科技有限公司	1	1
苏州棱镜七彩信息科技有限公司	1	1
海南神州希望网络有限公司	1	1
京东探索研究院信息安全实验室	1	1
西门子（中国）有限公司	1	0
联想集团	1	1
任子行网络技术股份有限公司	1	1
CNCERT 浙江分中心	10	10
CNCERT 贵州分中心	3	3
个人	1957	1957
报送总计	13632	9337

本周漏洞按类型和厂商统计

本周，CNVD 收录了 369 个漏洞。WEB 应用 179 个，应用程序 80 个，网络设备（交换机、路由器等网络端设备）60 个，数据库 23 个，操作系统 14 个，智能设备（物联网终端设备）12 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
WEB 应用	179
应用程序	80
网络设备（交换机、路由器等网络端设备）	60
数据库	23
操作系统	14
智能设备（物联网终端设备）	12
安全产品	1

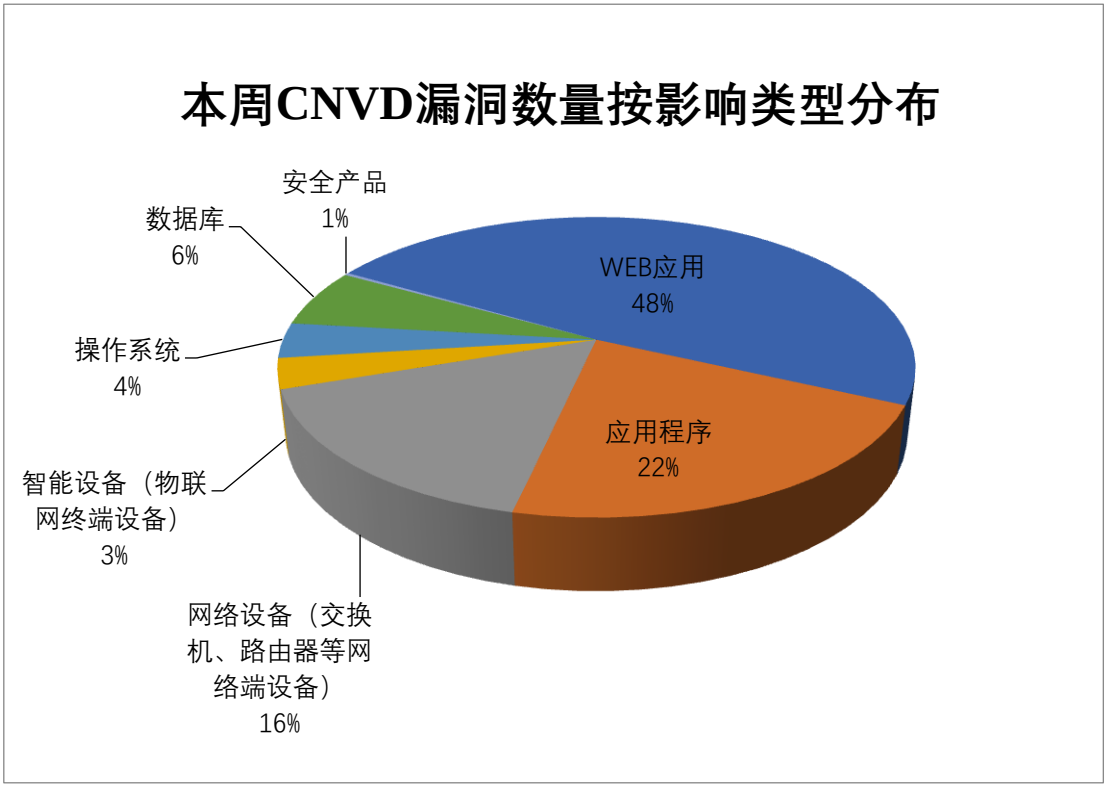

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Bentley Systems、WordPress、Oracle 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	Bentley Systems	21	6%
2	WordPress	20	5%
3	Oracle	18	5%
4	InHand Networks	12	3%
5	ASUS	12	3%
6	D-Link	12	3%
7	Google	12	3%
8	YottaDB	11	3%

9	ZOHO	10	3%
10	其他	241	66%

本周行业漏洞收录情况

本周，CNVD 收录了 63 个电信行业漏洞，8 个移动互联网行业漏洞，5 个工控行业漏洞（如下图所示）。其中，“DrayTek Vigor 远程命令注入漏洞、Wire 跨站脚本漏洞（CNVD-2022-31755）”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/

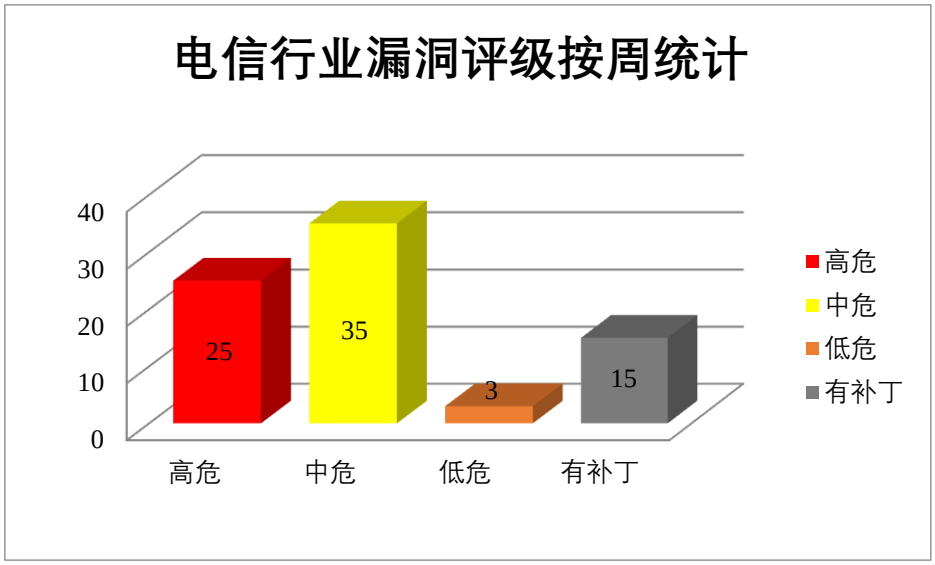

图 3 电信行业漏洞统计

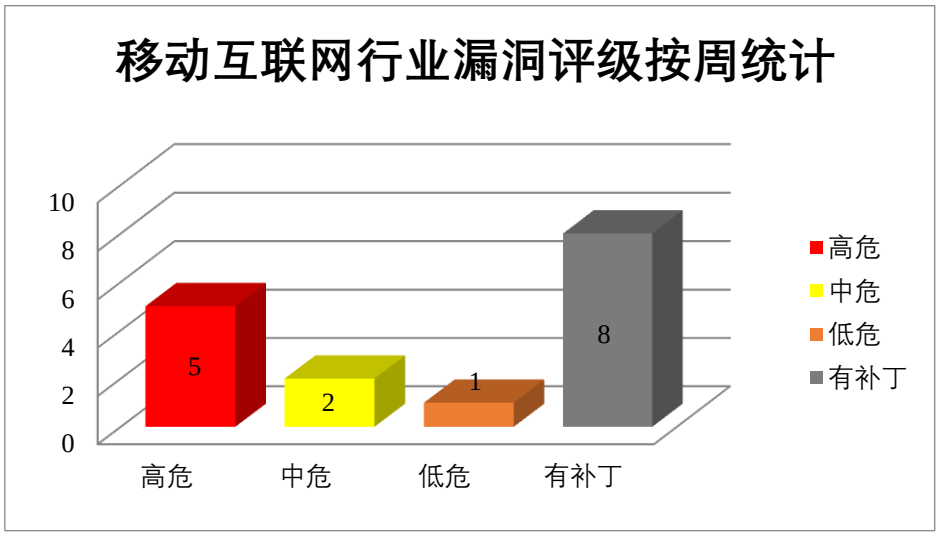

图 4 移动互联网行业漏洞统计

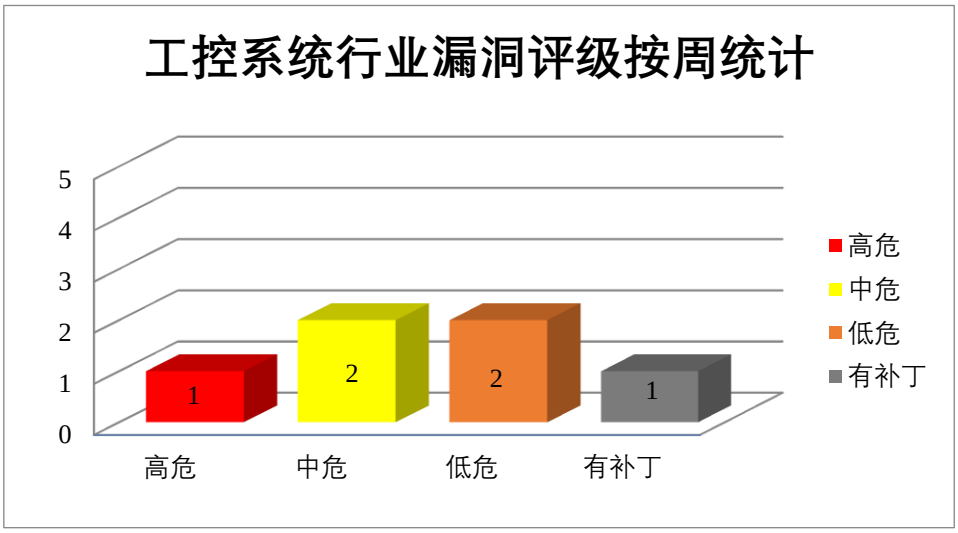

图 5 工控系统行业漏洞统计

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 Android 是美国谷歌（Google）公司的一套以 Linux 为基础的开源操作系统。Google Fscrypt 是美国谷歌（Google）公司的一个开源高级工具。用于管理 Linux 本机文件系统加密。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多个漏洞，攻击者可利用漏洞访问敏感信息，升级系统上的权限，执行任意代码等。

CNVD 收录的相关漏洞包括：Google Android 输入验证错误漏洞（CNVD-2022-31771、CNVD-2022-31845）、Google fscrypt 命令注入漏洞、Google Android 缓冲区溢出漏洞（CNVD-2022-31836、CNVD-2022-31840）、Google Chrome 输入验证错误漏洞（CNVD-2022-31839）、Google Android 权限许可和访问控制问题漏洞（CNVD-2022-31846、CNVD-2022-31844）。其中，除“Google Android 输入验证错误漏洞（CNVD-2022-31771、CNVD-2022-31836）、Google Chrome 输入验证错误漏洞（CNVD-2022-31839）”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-2022-31771

https://www.cnvd.org.cn/flaw/show/CNVD-2022-31832

https://www.cnvd.org.cn/flaw/show/CNVD-2022-31836

https://www.cnvd.org.cn/flaw/show/CNVD-2022-31840

https://www.cnvd.org.cn/flaw/show/CNVD-2022-31839

https://www.cnvd.org.cn/flaw/show/CNVD-2022-31846

https://www.cnvd.org.cn/flaw/show/CNVD-2022-31845

https://www.cnvd.org.cn/flaw/show/CNVD-2022-31844

2、 ASUS 产品安全漏洞

ASUS RT-AX56U 是中国台湾华硕（ASUS）公司的一款无线路由器。ASUS RT-AC86U 是中国华硕（ASUS）公司的一款双频 Wi-Fi 路由器。ASUS RT-AC56U 是中国华硕（ASUS）公司的一款双频 Wi-Fi 路由器。MyASUS 是中国华硕（ASUS）公司的一个华硕官方 PC 应用程序。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞注入任意 SQL 代码来读取、修改和删除数据库，执行任意代码，执行任意操作或中断服务等。

CNVD 收录的相关漏洞包括：ASUS RT-AX56U update_json 函数路径遍历漏洞、ASUS RT-AC56U 堆缓冲区溢出漏洞、ASUS RT-AC86U 输入验证错误漏洞、ASUS RT-AX56U 堆栈缓冲区溢出漏洞、ASUS RT-AX56U SQL 注入漏洞、ASUS RT-AX56U update_PLC/PORT 文件路径遍历漏洞、ASUS MyASUS 权限提升漏洞、ASUS RT-AC86U 命令注入漏洞。其中，“ASUS MyASUS 权限提升漏洞”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-2022-31516

https://www.cnvd.org.cn/flaw/show/CNVD-2022-31521

https://www.cnvd.org.cn/flaw/show/CNVD-2022-31520

https://www.cnvd.org.cn/flaw/show/CNVD-2022-31519

https://www.cnvd.org.cn/flaw/show/CNVD-2022-31518

https://www.cnvd.org.cn/flaw/show/CNVD-2022-31517

https://www.cnvd.org.cn/flaw/show/CNVD-2022-31525

https://www.cnvd.org.cn/flaw/show/CNVD-2022-31522

3、 ZOHO 产品安全漏洞

ZOHO ManageEngine ServiceDesk Plus（SDP）是美国卓豪（ZOHO）公司的一套基于 ITIL 架构的 IT 服务管理软件。该软件集成了事件管理、问题管理、资产管理 IT 项目管理、采购与合同管理等功能模块。ZOHO ManageEngine Adaudit Plus 是美国 Zoho Corporation 公司的用于简化审计、证明合规性和检测威胁。ZOHO ManageEngine Netflow Analyzer 是美国卓豪（ZOHO）公司的一套基于 Web 的带宽监控工具。该产品主要用于带宽监控和流量分析。ZOHO ManageEngine SharePoint Manager Plus 是美国卓豪（ZOHO）公司的一个完整管理和审计解决方案。ZOHO ManageEngine Desktop Central（DC）是美国卓豪（ZOHO）公司的一套桌面管理解决方案。该方案包含软件分发、补丁管理、系统配置、远程控制等功能模块，可对桌面机以及服务器管理的整个生命周期提供支持。ZOHO ManageEngine Key Manager Plus 是卓豪（ZOHO）公司的一

套基于 WEB 的 SSH 秘钥管理解决方案。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供应商货币详细信息，在集成产品上进行经过身份验证的权限提升，进行远程代码执行等。

CNVD 收录的相关漏洞包括：ZOHO ManageEngine ServiceDesk Plus 信息泄露漏洞（CNVD-2022-29863）、Zoho ManageEngine ADAudit Plus 远程代码执行漏洞、Zoho ManageEngine ADAudit Plus 权限提升漏洞、Zoho ManageEngine Netflow Analyzer Professional 跨站脚本漏洞、ZOHO ManageEngine SharePoint Manager Plus 权限提升漏洞、ZOHO ManageEngine SharePoint Manager Plus 授权问题漏洞、ZOHO ManageEngine Desktop Central 信息泄露漏洞（CNVD-2022-29876）、ZOHO ManageEngine Key Manager Plus 信息泄露漏洞。其中，“Zoho ManageEngine ADAudit Plus 远程代码执行漏洞、ZOHO ManageEngine SharePoint Manager Plus 权限提升漏洞、ZOHO ManageEngine SharePoint Manager Plus 授权问题漏洞”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-2022-29863
https://www.cnvd.org.cn/flaw/show/CNVD-2022-29866
https://www.cnvd.org.cn/flaw/show/CNVD-2022-29864
https://www.cnvd.org.cn/flaw/show/CNVD-2022-29867
https://www.cnvd.org.cn/flaw/show/CNVD-2022-29874
https://www.cnvd.org.cn/flaw/show/CNVD-2022-29873
https://www.cnvd.org.cn/flaw/show/CNVD-2022-29876
https://www.cnvd.org.cn/flaw/show/CNVD-2022-29875

4、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。MySQL Server 是其中的一个数据库服务器组件。MySQL Connectors 是其中的一个连接使用 MySQL 的应用程序的驱动程序。Oracle Commerce 是美国甲骨文（Oracle）公司的一套电子商务解决方案。Oracle Virtualization 和 Oracle VM VirtualBox 都是美国甲骨文（Oracle）公司的产品。Oracle Virtualization 是一套虚拟化解决方案。该产品用于统一管理从应用程序到磁盘的整个硬件和软件体系，可实现从桌面到数据中心的虚拟化。VM VirtualBox 是其中的一个虚拟机组件。Oracle VM VirtualBox 是一款虚拟机管理软件。Oracle Solaris 是美国甲骨文（Oracle）公司的一套 UNIX 操作系统。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞导致 MySQL Server 挂起或频繁重复崩溃（完全 DOS），执行 Oracle VM VirtualBox 的基础设施来破坏 Oracle VM VirtualBox 等。

CNVD 收录的相关漏洞包括：Oracle MySQL 输入验证错误漏洞（CNVD-2022-31681、CNVD-2022-31688、CNVD-2022-31687、CNVD-2022-31686）、Oracle Virtualizati

on 和 Oracle VM VirtualBox 输入验证错误漏洞（CNVD-2022-31685）、Oracle Commerce 输入验证错误漏洞（CNVD-2022-31684）、Oracle Virtualization 和 Oracle VM VirtualBox 输入验证错误漏洞（CNVD-2022-31683）、Oracle Solaris 拒绝服务漏洞（CNVD-2022-31682）。其中，“Oracle Commerce 输入验证错误漏洞（CNVD-2022-31684）”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-2022-31681
https://www.cnvd.org.cn/flaw/show/CNVD-2022-31684
https://www.cnvd.org.cn/flaw/show/CNVD-2022-31683
https://www.cnvd.org.cn/flaw/show/CNVD-2022-31682
https://www.cnvd.org.cn/flaw/show/CNVD-2022-31686
https://www.cnvd.org.cn/flaw/show/CNVD-2022-31685
https://www.cnvd.org.cn/flaw/show/CNVD-2022-31688
https://www.cnvd.org.cn/flaw/show/CNVD-2022-31687

5、Linux kernel 资源管理错误漏洞（CNVD-2022-31767）

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，Linux kernel 被披露存在资源管理错误漏洞。攻击者可利用该漏洞造成拒绝服务。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-2022-31767

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-2022-30456	Sourcecodester Attendance and Payroll 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://www.sourcecodester.com/sites/default/files/download/oretnom23/apsystem.zip
CNVD-2022-30455	Sourcecodester Attendance and Payroll System 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://www.sourcecodester.com/sites/default/files/download/oretnom23/apsystem.zip
CNVD-2022-30674	Microsoft Windows Remote Procedure Call Runtime 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://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-26809

CNVD-2022-30773	Atom.CMS SQL 注入漏洞（CNVD-2022-30773）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/thedigicraft/Atom.CMS/issues/261
CNVD-2022-30772	Atom.CMS SQL 注入漏洞（CNVD-2022-30772）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/thedigicraft/Atom.CMS/issues/262
CNVD-2022-30776	Atom.CMS SQL 注入漏洞（CNVD-2022-30776）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/thedigicraft/Atom.CMS/issues/259
CNVD-2022-30775	Atom.CMS 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/thedigicraft/Atom.CMS/issues/260
CNVD-2022-30774	Atom.CMS SQL 注入漏洞（CNVD-2022-30774）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/thedigicraft/Atom.CMS/issues/263
CNVD-2022-30778	CSZ CMS SQL 注入漏洞（CNVD-2022-30778）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/cskaza/cszcms/issues/45
CNVD-2022-30777	CSZ CMS SQL 注入漏洞（CNVD-2022-30777）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/cskaza/cszcms/issues/42

小结：本周，Google 产品被披露存在多个漏洞，攻击者可利用漏洞访问敏感信息，升级系统上的权限，执行任意代码等。此外，ASUS、ZOHO、Oracle 等多款产品被披露存在多个漏洞，攻击者可利用漏洞注入任意 SQL 代码来读取、修改和删除数据库，执行任意代码，执行任意操作或中断服务等。另外，Linux kernel 被披露存在资源管理错误漏洞。攻击者可利用该漏洞造成拒绝服务。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、AeroCMS 跨站脚本漏洞（CNVD-2022-30784）

验证描述

AeroCMS 是美国 AeroCMS 公司的一个内容管理系统。

AeroCMS v0.0.1 版本存在跨站脚本漏洞，攻击者可利用该漏洞通过注入“评论”文本字段的特制有效负载执行任意 Web 脚本或 HTML。

验证信息

POC 链接：https://github.com/D4rkP0w4r/AeroCMS-Comment-Stored_XSS-Poc

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2022-30784

信息提供者

深信服科技股份有限公司

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. QNAP 固件更新修复其 NAS 中的 Apache HTTP 漏洞

QNAP 警告用户更新他们的 NAS 固件，以修复上个月在 Apache HTTP 服务器中解决的 Apache HTTP 漏洞。

参考链接：https://securityaffairs.co/wordpress/130481/hacking/qnap-nas-firmware-fix-apache-http-flaws.html

2. “Hack DHS”漏洞猎人在 DHS 系统中发现 122 个安全漏洞

美国国土安全部 (DHS) 今天透露，参与其“Hack DHS”漏洞赏金计划的漏洞赏金猎人在外部 DHS 系统中发现了 122 个安全漏洞，其中 27 个被评为严重严重性。

参考链接：https://www.bleepingcomputer.com/news/security/hack-dhs-bug-hunters-find-122-security-flaws-in-dhs-systems/

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