国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2022 年 08 月 15 日-2022 年 08 月 21 日 **2022 年第 33 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 558 个，其中高危漏洞 163 个、中危漏洞 298 个、低危漏洞 97 个。漏洞平均分值为 5.63。本周收录的漏洞中，涉及 0day 漏洞 317 个（占 57%），其中互联网上出现“Air Cargo Management System SQL 注入漏洞（CNVD-2022-58095）、Simple Client Management System SQL 注入漏洞（CNVD-2022-57772）”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漏洞总数 18020 个，与上周（5952 个）环比增加 203%。

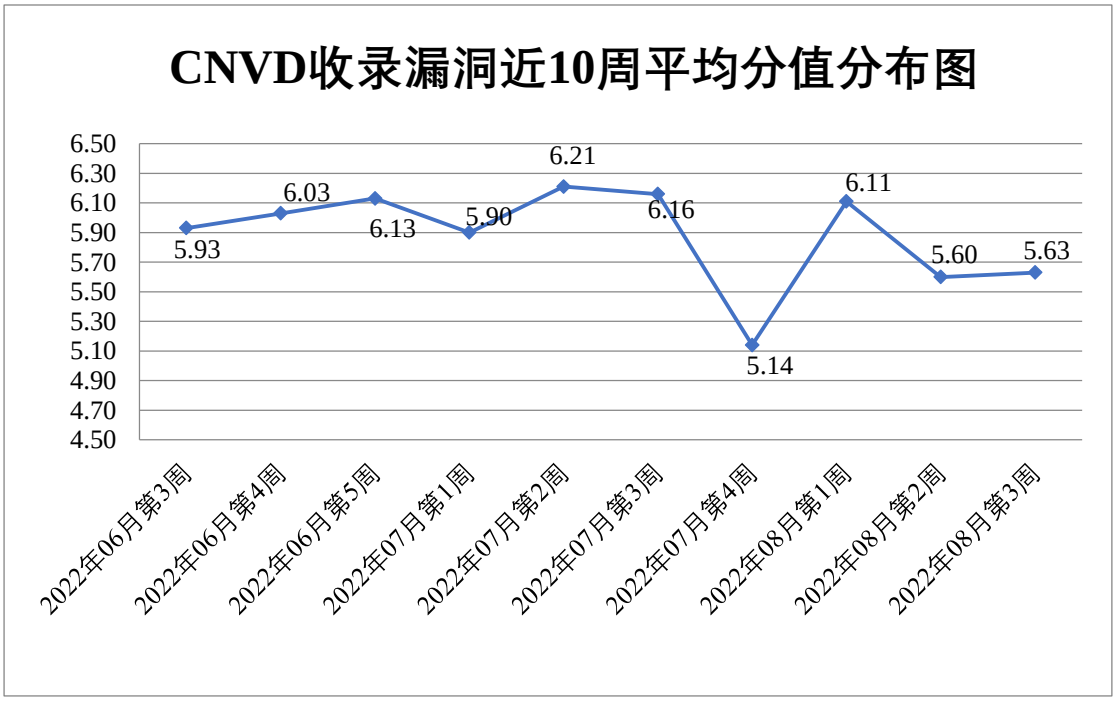

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 20 起，向基础电

信企业通报漏洞事件 34 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 434 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 86 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：

重庆佰鼎科技有限公司、中资国民科技有限公司、中山市蓝图网络科技有限公司、正方软件股份有限公司、浙江大华技术股份有限公司、长沙友点软件科技有限公司、友讯电子设备（上海）有限公司、用友网络科技股份有限公司、业乔投资（集团）有限公司、兄弟（中国）商业有限公司、新天科技股份有限公司、西安微光软件科技有限公司、西安极通软件信息科技有限公司、武汉舜通智能科技有限公司、武汉金同方科技有限公司、武汉达梦数据库股份有限公司、无锡信捷电气股份有限公司、温州互引信息技术有限公司、维沃移动通信（深圳）有限公司、完美（中国）有限公司、统信软件技术有限公司、天津星通九恒科技有限公司、天津神舟通用数据技术有限公司、腾讯安全应急响应中心、台州华顶网络技术有限公司、索尼（中国）有限公司、苏州酷曼软件技术有限公司、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、四创科技有限公司、四川迅睿云软件开发有限公司、神州数码信息服务股份有限公司、深圳中维世纪科技有限公司、深圳智慧光迅信息技术有限公司、深圳市乙辰科技股份有限公司、深圳市迅捷通信技术有限公司、深圳市小猫信息技术有限公司、深圳市同为数码科技股份有限公司、深圳市深海捷科技有限公司、深圳市明源云科技有限公司、深圳市蓝凌软件股份有限公司、深圳市吉祥腾达科技有限公司、深圳市和为顺网络技术有限公司、深圳市皓峰通讯技术有限公司、深圳市必联电子有限公司、深圳科士达科技股份有限公司、上海卓卓网络科技有限公司、上海盈策信息技术有限公司、上海移品信息技术有限公司、上海寻梦信息技术有限公司、上海晓材科技有限公司、上海上业信息科技股份有限公司、上海三少变美网络科技有限公司、上海赛连信息科技有限公司、上海茸易科技有限公司、上海青枣网络科技有限公司、上海穆云智能科技有限公司、上海亘岩网络科技有限公司、上海泛微网络科技股份有限公司、上海顶想信息科技有限公司、上海冰峰计算机网络技术有限公司、上海艾泰科技有限公司、山西建投物资贸易有限公司、山石网科通信技术股份有限公司、山东山大电力技术股份有限公司、三星（中国）投资有限公司、润申信息科技（上海）有限公司、睿因科技（深圳）有限公司、瑞斯康达科技发展股份有限公司、普联技术有限公司、南京管鲍科技发展有限公司、南京帆软软件有限公司、南昌蓝智科技有限公司、明腾网络股份有限公司、迈普通信技术股份有限公司、联想（北京）有限公司、乐视网信息技术（北京）股份有限公司、昆明市网翼通科技有限公司、江西铭软科技有限公司、江苏易安联网络技术有限公司、江苏曼荼罗软件股份有限公司、江苏金智教育信息股份有限公司、佳能（中国）有限公司、济南驰骋信息技术有限公司、吉翁

电子（深圳）有限公司、湖南一唯信息科技有限公司、湖南羊驼教育科技有限公司、湖南翱云网络科技有限公司、洪湖尔创网联信息技术有限公司、恒锋信息科技股份有限公司、浩海网络科技股份有限公司、杭州可道云网络有限公司、杭州海康威视数字技术股份有限公司、海南有趣科技有限公司、海南驰豹科技有限公司、哈尔滨伟成科技有限公司、桂林崇胜网络科技有限公司、广州红迅软件有限公司、广东世纪信通网络科技有限公司、阜阳市心品网络科技有限公司、福建升腾资讯有限公司、福建福昕软件开发股份有限公司、东软集团股份有限公司、戴尔（中国）有限公司、大连华天软件有限公司、成都零起飞科技有限公司、成都光大网络科技有限公司、畅捷通信息技术股份有限公司、博世（中国）投资有限公司、北京中商惠民智盛科技有限公司、北京中庆纳博信息技术有限公司、北京中创视讯科技有限公司、北京致远互联软件股份有限公司、北京芝士科技有限公司、北京元年科技股份有限公司、北京星网锐捷网络技术有限公司、北京小米科技有限责任公司、北京微瑞集智科技有限公司、北京网康科技有限公司、北京通通易联科技有限公司、北京通达信科科技有限公司、北京天融信科技有限公司、北京素玄网络科技有限公司、北京素玄科技有限公司、北京数字政通科技股份有限公司、北京施惠特科技有限责任公司、北京七陌科技有限公司、北京派网软件有限公司、北京露营者房车科技有限公司、北京九思协同软件有限公司、北京金和网络股份有限公司、北京极科极客科技有限公司、北京华宇信息技术有限公司、北京观复文化有限公司、北京抖音信息服务有限公司、北京弹幕网络科技有限公司、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、安徽微同科技有限公司、安徽省通源环境节能股份有限公司、安徽庆宇光电科技有限公司、安徽青柿信息科技有限公司、阿帕数字技术有限公司 、东方财富安全应急响应中心、点雅互动、信呼、华夏 ERP、ZZCMS、Lexmark 和 Catfish CMS。

本周，CNVD 发布了《关于 Apple 操作系统越界写入漏洞和 Apple WebKit 越界写入漏洞的安全公告》。详情参见 CNVD 网站公告内容。

https://www.cnvd.org.cn/webinfo/show/8011

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、北京数字观星科技有限公司、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、新华三技术有限公司等单位报送公开收集的漏洞数量较多。北京华顺信安信息技术有限公司、中国电信股份有限公司网络安全产品运营中心、贵州泰若数字科技有限公司、河南东方云盾信息技术有限公司、奇安星城网络安全运营服务（长沙）有限公司、山石网科通信技术股份有限公司、河南信安世纪科技有限公司、浙江木链物联网科技有限公司、浙江大学控制科学与工程学院、河南灵创电子科技有限公司、西藏熙安信息技术有限责任公司、福建省海峡信息技术有限公司、江西和尔惠信息技术有限公司、广州安亿信软件科技有限

公司、上海纽盾科技股份有限公司、北京山石网科信息技术有限公司、北京众安天下科技有限公司、中国—东盟信息港股份有限公司、苏州棱镜七彩信息科技有限公司、墨菲未来科技（北京）有限公司、广州易东信息安全技术有限公司、工业和信息化部电子第五研究所、广电奇安网络科技（重庆）有限公司、麒麟软件有限公司、云南联创网安科技有限公司、杭州默安科技有限公司、北京机沃科技有限公司、玄蜂安全团队、河南天祺信息安全技术有限公司、北京快手科技有限公司、平安银河实验室及其他个人白帽子向 CNVD 提交了 18020 个以事件型漏洞为主的原创漏洞，其中包括奇安信网神（补天平台）、三六零数字安全科技集团有限公司、斗象科技（漏洞盒子）和上海交大向 CNVD 共享的白帽子报送的 16096 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
奇安信网神（补天平台）	12527	12527
三六零数字安全科技集团有限公司	2365	2365
深信服科技股份有限公司	1251	2
斗象科技（漏洞盒子）	909	909
北京数字观星科技有限公司	574	0
杭州安恒信息技术股份有限公司	465	302
北京神州绿盟科技有限公司	398	2
新华三技术有限公司	339	0
上海交大	295	295
安天科技集团股份有限公司	224	0
北京启明星辰信息安全技术有限公司	121	59
北京天融信网络安全技术有限公司	117	21
恒安嘉新（北京）科技股份公司	115	0
天津市国瑞数码安全系统股份有限公司	115	0
南京众智维信息科技有限公司	75	75
内蒙古云科数据服务股份有限公司	24	24
中国电信集团系统集	23	0

成有限责任公司		
京东科技信息技术有限公司	14	14
北京长亭科技有限公司	8	8
南京联成科技发展股份有限公司	8	8
西安四叶草信息技术有限公司	4	4
北京知道创宇信息技术有限公司	4	2
内蒙古奥创科技有限公司	3	3
远江盛邦（北京）网络安全科技股份有限公司	3	3
北京智游网安科技有限公司	2	2
北京华顺信安信息技术有限公司	322	2
中国电信股份有限公司网络安全产品运营中心	203	203
贵州泰若数字科技有限公司	117	117
河南东方云盾信息技术有限公司	50	50
奇安星城网络安全运营服务（长沙）有限公司	30	30
山石网科通信技术股份有限公司	23	23
杭州迪普科技股份有限公司	15	0
河南信安世纪科技有限公司	8	8
浙江木链物联网科技有限公司	7	7
浙江大学控制科学与工程学院	4	4
河南灵创电子科技有限公司	4	4
西藏熙安信息技术有	4	4

限责任公司		
福建省海峡信息技术有限公司	4	4
江西和尔惠信息技术有限公司	3	3
广州安亿信软件科技有限公司	3	3
上海纽盾科技股份有限公司	3	3
北京山石网科信息技术有限公司	3	3
北京众安天下科技有限公司	2	2
中国—东盟信息港股份有限公司	2	2
苏州棱镜七彩信息科技有限公司	2	2
墨菲未来科技（北京）有限公司	1	1
广州易东信息安全技术有限公司	1	1
工业和信息化部电子第五研究所	1	1
广电奇安网络科技（重庆）有限公司	1	1
麒麟软件有限公司	1	1
云南联创网安科技有限公司	1	1
杭州默安科技有限公司	1	1
北京机沃科技有限公司	1	1
玄蜂安全团队	1	1
河南天祺信息安全技术有限公司	1	1
北京快手科技有限公司	1	1
平安银河实验室	1	1
个人	909	909
报送总计	21713	18020

本周漏洞按类型和厂商统计

本周，CNVD 收录了 558 个漏洞。WEB 应用 314 个，应用程序 130 个，网络设备（交换机、路由器等网络端设备）68 个，操作系统 19 个，安全产品 18 个，智能设备（物联网终端设备）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	314
应用程序	130
网络设备（交换机、路由器等网络端设备）	68
操作系统	19
安全产品	18
智能设备（物联网终端设备）	9

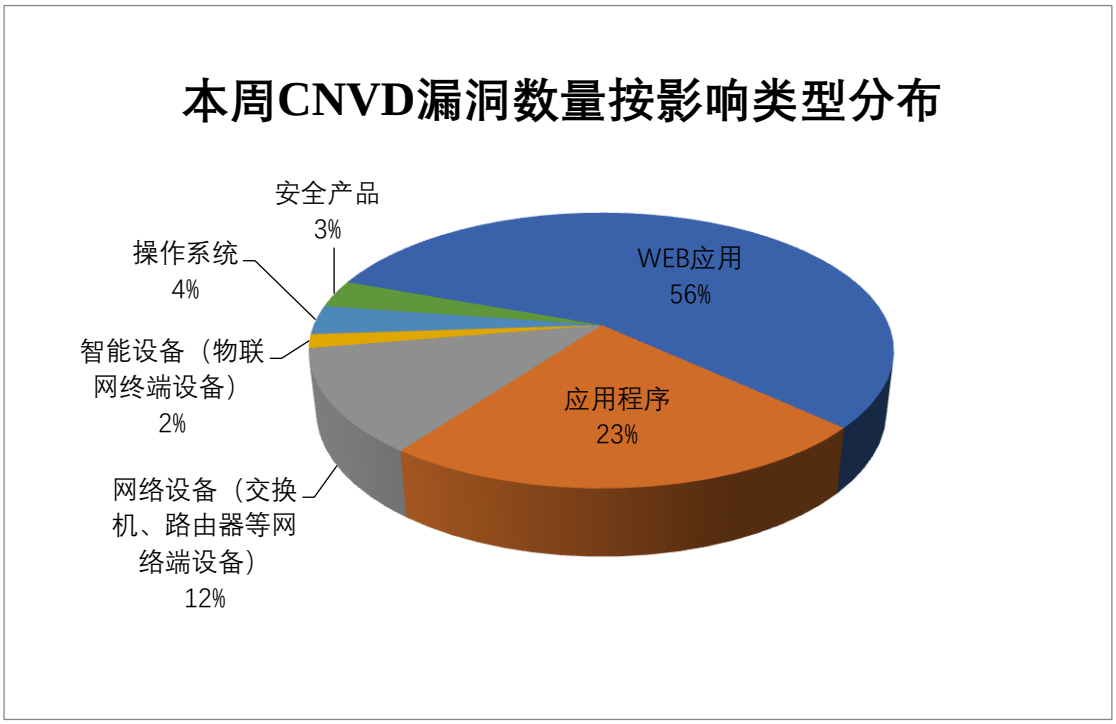

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 WordPress、Zoneminder、SAP 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	WordPress	70	13%
2	Zoneminder	24	4%
3	SAP	23	4%
4	Jenkins	21	4%
5	Microsoft	13	2%

6	D-Link	13	2%
7	Simple Client Management System	11	2%
8	IBM	10	2%
9	Joomla!	10	2%
10	其他	363	65%

本周行业漏洞收录情况

本周，CNVD 收录了 60 个电信行业漏洞，25 个移动互联网行业漏洞，9 个工控行业漏洞（如下图所示）。其中，“Google Android Modem 组件拒绝服务漏洞、Apple 操作系统越界写入漏洞”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/

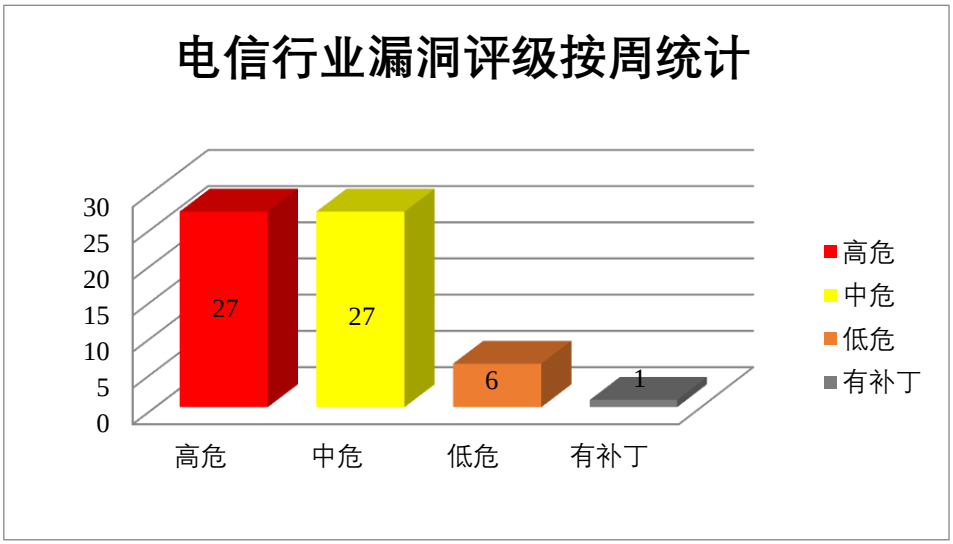

图 3 电信行业漏洞统计

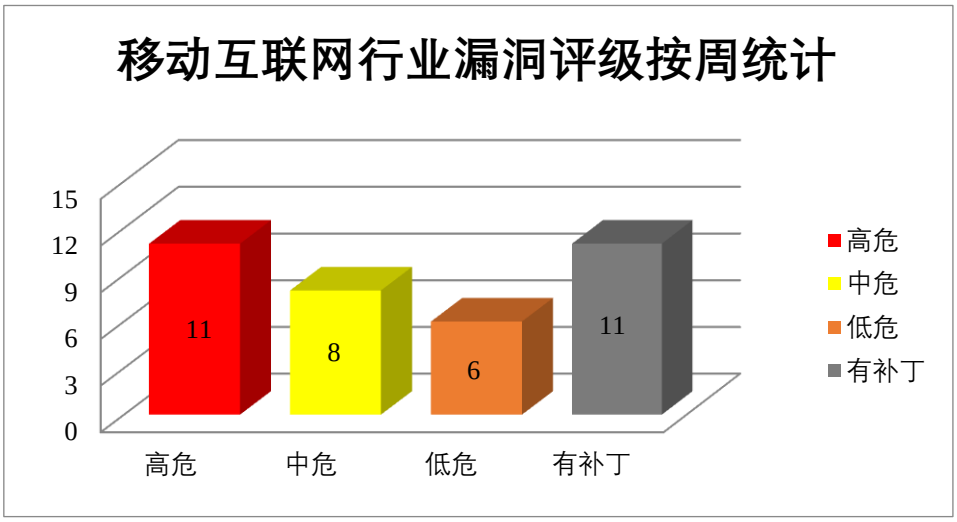

图 4 移动互联网行业漏洞统计

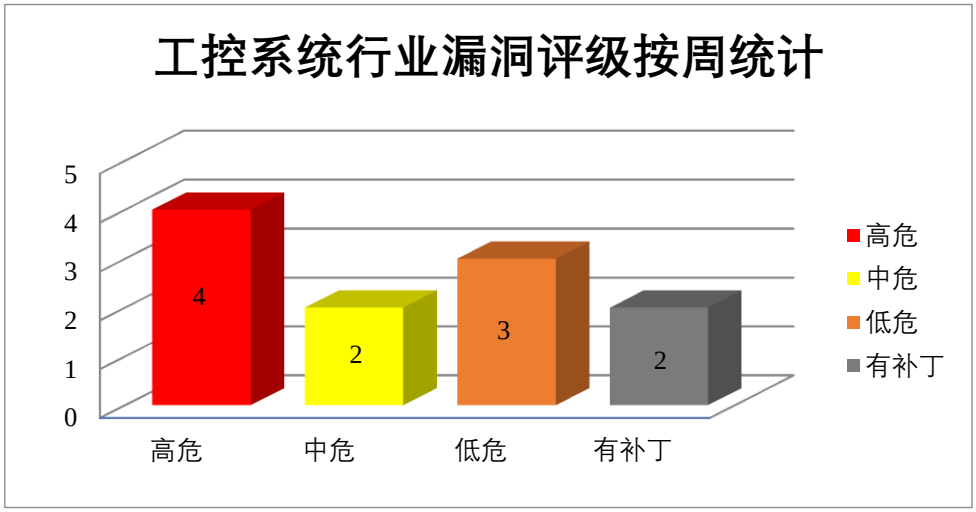

图 5 工控系统行业漏洞统计

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、 Microsoft 产品安全漏洞

Microsoft Azure Site Recovery 是美国微软（Microsoft）公司的一种站点恢复（DRaaS），用于云和混合云架构。本周，上述产品被披露存在权限提升漏洞，攻击者可利用漏洞在系统上获得提升的权限。

CNVD 收录的相关漏洞包括：Microsoft Azure Site Recovery 权限提升漏洞（CNVD-2022-57194、CNVD-2022-57193、CNVD-2022-57197、CNVD-2022-57196、CNVD-2022-57195、CNVD-2022-57201、CNVD-2022-57200、CNVD-2022-57199）。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-2022-57194
https://www.cnvd.org.cn/flaw/show/CNVD-2022-57193
https://www.cnvd.org.cn/flaw/show/CNVD-2022-57197
https://www.cnvd.org.cn/flaw/show/CNVD-2022-57196
https://www.cnvd.org.cn/flaw/show/CNVD-2022-57195
https://www.cnvd.org.cn/flaw/show/CNVD-2022-57201
https://www.cnvd.org.cn/flaw/show/CNVD-2022-57200
https://www.cnvd.org.cn/flaw/show/CNVD-2022-57199

2、SAP 产品安全漏洞

SAP NetWeaver Enterprise Portal 是一个 SAP NetWeaver 的 Web 前端组件。SAP SuccessFactors 是德国思爱普（SAP）公司的一个基于云的 Hcm 软件应用程序。SAP Business One 是德国思爱普（SAP）公司的一套企业管理软件。该软件包括财务管理、运营管理和人力资源管理等功能。SAP BusinessObjects BW Publisher Service 是德国 SAP 公司的一种模型驱动数据仓库产品。SAP Business Objects 是德国 SAP 公司的一个商业智能套件。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞获得敏感信息、查看或修改信息、提升权限、执行拒绝服务攻击，使系统暂时无法运行等。

CNVD 收录的相关漏洞包括：SAP NetWeaver Enterprise Portal 跨站脚本漏洞（CNVD-2022-56942、CNVD-2022-56941）、SAP SuccessFactors 权限提升漏洞、SAP Business One 拒绝服务漏洞、SAP Business One 代码注入漏洞（CNVD-2022-56957）、SAP BusinessObjects BW Publisher Service 权限提升漏洞、SAP BusinessObjects Business Intelligence Platform SQL 注入漏洞、SAP Business One 信息泄露漏洞（CNVD-2022-56961）。其中，“SAP SuccessFactors 权限提升漏洞”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-2022-56942
https://www.cnvd.org.cn/flaw/show/CNVD-2022-56941
https://www.cnvd.org.cn/flaw/show/CNVD-2022-56955
https://www.cnvd.org.cn/flaw/show/CNVD-2022-56960
https://www.cnvd.org.cn/flaw/show/CNVD-2022-56957
https://www.cnvd.org.cn/flaw/show/CNVD-2022-56963
https://www.cnvd.org.cn/flaw/show/CNVD-2022-56962
https://www.cnvd.org.cn/flaw/show/CNVD-2022-56961

3、IBM 产品安全漏洞

IBM CICS TX Advanced 是美国 IBM 公司的一个综合的、单一的事务运行时包。可以为独立应用程序提供云原生部署模型。IBM DataPower Gateway 是美国 IBM 公司

的一套专门为移动、云、应用编程接口（API）、网络、面向服务架构（SOA）、B2B和云工作负载而设计的安全和集成平台。该平台可利用专用网关平台跨渠道保护、集成和优化访问。IBM Robotic Process Automation 是美国 IBM 公司的一种机器人流程自动化产品。可帮助您以传统 RPA 的轻松和速度大规模自动化更多业务和 IT 流程。IBM QRadar SIEM 是美国 IBM 公司的一套利用安全智能保护资产和信息远离高级威胁的解决方案。该方案提供对整个 IT 架构范围进行监督、生成详细的数据访问和用户活动报告等功能。IBM Engineering Lifecycle Optimization（ELO）是美国 IBM 公司的工程生命周期管理 (ELM) 产品组合的扩展。它们可以更轻松地收集和分析整个开发环境中的数据，以做出更好的决策。自动化报告以确保整个组织拥有优化开发所需的信息，定义可以帮助您的扩展团队采用和遵循最佳实践的流程，与第三方工具接口以自定义您的开发环境。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，造成应用拒绝服务等。

CNVD 收录的相关漏洞包括：IBM CICS TX 跨站请求伪造漏洞、IBM DataPower Gateway 服务器端请求伪造漏洞（CNVD-2022-56971）、IBM DataPower Gateway XML 外部实体注入漏洞（CNVD-2022-56970）、IBM Robotic Process Automation 信息泄露漏洞（CNVD-2022-56974）、IBM Robotic Process Automation 权限提升漏洞、IBM DataPower Gateway 跨站脚本漏洞（CNVD-2022-56972）、IBM QRadar SIEM 拒绝服务漏洞（CNVD-2022-56976）、IBM Engineering Lifecycle Optimization 信息泄露漏洞。其中，“IBM CICS TX 跨站请求伪造漏洞、IBM DataPower Gateway 服务器端请求伪造漏洞（CNVD-2022-56971）、IBM DataPower Gateway XML 外部实体注入漏洞（CNVD-2022-56970）、IBM Robotic Process Automation 权限提升漏洞”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-2022-56968
https://www.cnvd.org.cn/flaw/show/CNVD-2022-56971
https://www.cnvd.org.cn/flaw/show/CNVD-2022-56970
https://www.cnvd.org.cn/flaw/show/CNVD-2022-56974
https://www.cnvd.org.cn/flaw/show/CNVD-2022-56973
https://www.cnvd.org.cn/flaw/show/CNVD-2022-56972
https://www.cnvd.org.cn/flaw/show/CNVD-2022-56976
https://www.cnvd.org.cn/flaw/show/CNVD-2022-56975

4、 Jenkins 产品安全漏洞

Jenkins 和 Jenkins Plugin 都是 Jenkins 开源的产品。Jenkins 是一个应用软件。一个开源自动化服务器 Jenkins 提供了数百个插件来支持构建，部署和自动化任何项目。Jenkins Plugin 是一个应用软件。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞

向指定的 URL 发送 HTTP 请求、创建和删除 XPath 表达式、获取敏感信息等。

CNVD 收录的相关漏洞包括：Jenkins Recipe Plugin XML 外部实体注入漏洞、Jenkins Recipe Plugin 跨站请求伪造漏洞、Jenkins RocketChat Notifier Plugin 信息泄露漏洞、Jenkins Skype notifier Plugin 信息泄露漏洞、Jenkins RQM Plugin 信息泄露漏洞、Jenkins XPath Configuration Viewer Plugin 授权问题漏洞、Jenkins Plugin requests-plugin 授权问题漏洞、Jenkins XebiaLabs XL Release Plugin 授权问题漏洞（CNVD-2022-58430）。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-2022-56925
https://www.cnvd.org.cn/flaw/show/CNVD-2022-56926
https://www.cnvd.org.cn/flaw/show/CNVD-2022-58416
https://www.cnvd.org.cn/flaw/show/CNVD-2022-58419
https://www.cnvd.org.cn/flaw/show/CNVD-2022-58418
https://www.cnvd.org.cn/flaw/show/CNVD-2022-58422
https://www.cnvd.org.cn/flaw/show/CNVD-2022-58425
https://www.cnvd.org.cn/flaw/show/CNVD-2022-58430

5、TP-LINK TL-R473G 远程代码执行漏洞

TP-LINK TL-R473G 是中国普联（TP-LINK）公司的一款千兆企业 VPN 路由器。本周，TP-LINK TL-R473G 被披露存在远程代码执行漏洞。攻击者可利用该漏洞通过特制的数据包执行远程代码。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-2022-56954

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：https://www.cnvd.org.cn/flaw/list

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-2022-57605	Google Android 权限提升漏洞（CNVD-2022-57605）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://source.android.com/security/bulletin/pixel/2022-07-01
CNVD-2022-58234	GLPI SQL 注入漏洞（CNVD-2022-58234）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/glpi-project/glpi-inventory-plugin/security/advisories/GHSA-q6m7-h6rj-5wmw
CNVD-2022-58398	Google Android Modem 组件拒绝服务漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：

			https://source.android.com/security/bulletin/pixel/2022-06-01?hl=en
CNVD-2022-58406	Adobe FrameMaker 资源管理错误漏洞（CNVD-2022-58406）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://helpx.adobe.com/security/products/framemaker/apsb22-42.html
CNVD-2022-58403	Google Android 代码执行漏洞（CNVD-2022-58403）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://source.android.com/security/bulletin/pixel/2022-06-01?hl=en
CNVD-2022-58423	Wordpress Plugin swfupload 对象注入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.openwall.com/lists/oss-security/2013/07/18/10
CNVD-2022-58431	GitLab 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://about.gitlab.com/update/
CNVD-2022-58458	Apple WebKit 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://support.apple.com/
CNVD-2022-57609	Google Android 远程代码执行漏洞（CNVD-2022-57609）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://source.android.com/security/bulletin/pixel/2022-07-01
CNVD-2022-58457	Apple 操作系统越界写入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://support.apple.com/

小结：本周，Microsoft 产品被披露存在权限提升漏洞，攻击者可利用漏洞在系统上获得提升的权限。此外，SAP、IBM、Jenkins 等多款产品被披露存在多个漏洞，攻击者可利用漏洞向指定的 URL 发送 HTTP 请求、获取敏感信息、提升权限、执行拒绝服务攻击，使系统暂时无法运行等。另外，TP-LINK TL-R473G 被披露存在远程代码执行漏洞。攻击者可利用该漏洞通过特制的数据包执行远程代码。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、Air Cargo Management System SQL 注入漏洞（CNVD-2022-58095）

验证描述

Air Cargo Management System 是一个空运货物管理系统。

Air Cargo Management System 1.0 版本存在 SQL 注入漏洞，该漏洞源于/acms/classes/Master.php?f=delete_cargo 缺少对于参数的过滤和转义，攻击者可利用该漏洞执行非法 SQL 命令窃取数据库敏感数据。

验证信息

POC 链接：https://github.com/k0xx11/bug_report/blob/main/vendors/oretnom23/air-cargo-management-system/SQLi-5.md

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2022-58094

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. iPhone、iMac 等产品存在安全漏洞

据美联社 20 日报道，美国苹果公司当地时间 17 日发布两份安全报告，两份报告披露，公司旗下智能手机 iPhone、平板电脑 iPad 和 iMac 电脑等产品存在安全漏洞。这些漏洞可能会让潜在的攻击者入侵用户设备、获得管理权限甚至完全控制设备并运行其中的应用软件。

参考链接：https://www.cnbeta.com/articles/tech/1306861.htm

2. Realtek 爆出安全漏洞，影响多款网络设备

Realtek 爆出安全漏洞，该漏洞影响到数百万台采用 Realtek RTL819x 系统芯片（SoC）的网络设备。该漏洞被追踪为 CVE-2022-27255，远程攻击者可以利用其破坏来自各种原始设备制造商（OEM）的易受攻击设备。

参考链接：https://www.bleepingcomputer.com/news/security/exploit-out-for-critical-realtek-flaw-affecting-many-networking-devices/

关于 CNVD

国家信息安全漏洞共享平台（China National Vulnerability Database，简称 CNVD）是由 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国家网络安全漏洞库，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，是我国计算机网络应急处理体系中的牵头单位。

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