国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2023 年 11 月 06 日-2023 年 11 月 12 日 **2023 年第 45 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 121 个、中危漏洞 209 个、低危漏洞 23 个。漏洞平均分值为 6.30。本周收录的漏洞中，涉及 0day 漏洞 299 个（占 85%），其中互联网上出现“Evolution CMS 跨站脚本漏洞（CNVD-2023-85602）、D-Link DAR-7000 mailrecvview.php 文件 SQL 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漏洞总数 23920 个，与上周（20305 个）环比增加 18%。

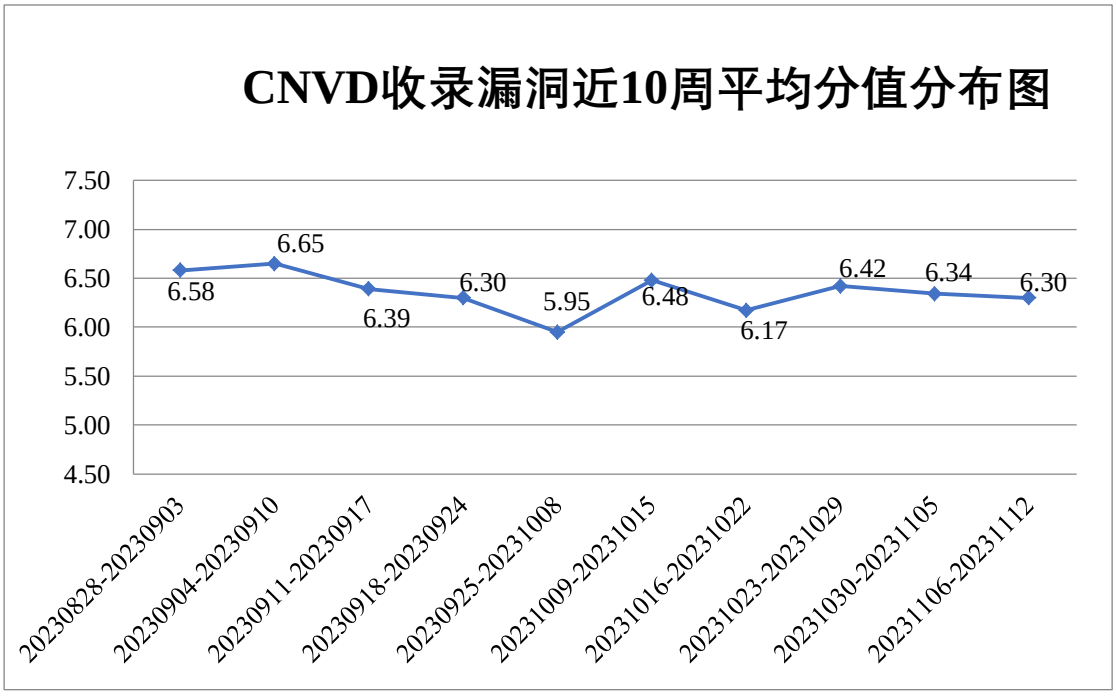

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 27 起，向基础电

信企业通报漏洞事件 18 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 1322 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 231 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 51 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：

自然阳光（上海）日用品有限公司、紫光股份有限公司、珠海派诺科技股份有限公司、珠海金山办公软件有限公司、重庆中联信息产业有限责任公司、重庆远秋科技股份有限公司、郑州金恒电子技术有限公司、正奇晟业（北京）科技有限公司、浙江中控自动化仪表有限公司、浙江花田网络有限公司、长沙市同迅计算机科技有限公司、长沙德尚网络科技有限公司、友讯电子设备（上海）有限公司、用友网络科技股份有限公司、永中软件股份有限公司、益丰大药房连锁股份有限公司、炫米信息技术（上海）有限公司、信呼、夏普科技（上海）有限公司、西安众邦网络科技有限公司、武汉中地数码科技有限公司、武汉达梦数据库股份有限公司、武汉初心科技有限公司、温州互引信息技术有限公司、网件（北京）网络技术有限公司、万兴科技集团股份有限公司、同望科技股份有限公司、天津天堰科技股份有限公司、太原易思软件技术有限公司、太原福莱瑞达物流设备科技有限公司、台达电子企业管理（上海）有限公司、随锐科技集团股份有限公司、四川汇学邦教育科技有限公司、施耐德电气（中国）有限公司、沈阳东软系统集成工程有限公司、沈阳宝石金卡信息技术股份有限公司、深圳中台威堡科技有限公司、深圳智慧光迅信息技术有限公司、深圳心颜科技有限责任公司、深圳搜豹网络有限公司、深圳市小泊科技有限公司、深圳市联软科技股份有限公司、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、深圳市惠尔顿信息技术有限公司、深圳市汉德网络科技有限公司、深圳市必联电子有限公司、深圳市安车检测股份有限公司、深圳古瑞瓦特能源股份有限公司、申瓯通信设备有限公司、上海卓卓网络科技有限公司、上海盈策信息技术有限公司、上海宜采软件科技有限公司、上海市金山区融媒体中心、上海时代光华教育发展有限公司、上海擎创信息技术有限公司、上海穆云智能科技有限公司、上海龙翊信息安全技术有限公司、上海捡人网络科技有限公司、上海国民集团健康科技有限公司、上海泛微网络科技股份有限公司、上海德米萨信息科技有限公司、山西复盛公药业集团有限公司医药分公司、山西复盛公健康药业有限公司、山石网科通信技术股份有限公司、山东家家悦集团有限公司、山东博硕自动化技术有限公司、厦门享联科技有限公司、厦门物之联智能科技有限公司、厦门四信通信科技有限公司、厦门科拓通讯技术股份有限公司、赛博爱思（上海）软件有限公司、启明信息技术股份有限公司、普联技术有限公司、朴和教育科技有限公司、南京数旗科技有限公司、南京访客乐网络科技有限公司、南京帆软软件有限公司、南京博森科技有限公司、墨菲未来科技(北京)有限公司、梅赛德斯-奔驰（中国）汽车销售有限公司、迈普通信技术股份有限公司、昆山

必捷必信息技术有限公司、快享医疗科技（上海）有限公司、金蝶软件（中国）有限公司、江苏鲲腾软件科技有限公司、吉翁电子（深圳）有限公司、惠普贸易（上海）有限公司、汇纳科技股份有限公司、湖南强智科技发展有限公司、湖南律豆网络科技有限公司、湖南汉坤实业有限公司、合勤科技股份有限公司、合力泰科技股份有限公司、杭州致梦科技有限公司、杭州指令集智能科技有限公司、杭州思福迪信息技术有限公司、杭州联核科技有限公司、杭州阔知网络科技有限公司、杭州海康威视数字技术股份有限公司、杭州恩软信息技术有限公司、海信集团有限公司、海南创业星空科技有限公司、广州友财信息科技有限公司、广州小橘灯信息科技有限公司、广州同聚成电子科技有限公司、广州思迈特软件有限公司、广州联享信息科技有限公司、广联达科技股份有限公司、广东合通建业科技股份有限公司、福州七分水智能科技有限公司、福建传爱网络科技有限公司、福建博思软件股份有限公司、菲尼克斯（中国）投资有限公司、帆软软件有限公司、都世通网络科技有限公司、东华软件股份公司、东方希望集团有限公司、东方网力科技股份有限公司、滴滴云计算有限公司、得实信息科技（深圳）有限公司、成都友加畅捷科技有限公司、成都江鼎禹丰科技有限公司、畅捷通信息技术股份有限公司、铂爵旅拍文化集团有限公司、北京中科聚网信息技术有限公司、北京中安网星科技有限责任公司、北京致远互联软件股份有限公司、北京雪迪龙科技股份有限公司、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、北京通达信科科技有限公司、北京硕人时代科技股份有限公司、北京神州视翰科技有限公司、北京上元信安技术有限公司、北京凯特伟业科技有限公司、北京火山引擎科技有限公司、北京华宇信息技术有限公司、北京北信源软件股份有限公司、北京佰才邦技术股份有限公司、北京百卓网络技术有限公司、北京 1039 科技发展有限公司、包头市昕科高创科技有限公司、奥琦玮信息科技（北京）有限公司、安元科技股份有限公司、安美世纪（北京）科技有限公司、安徽省庐江县金点子文化传媒有限责任公司、爱普生（中国）有限公司、阿里巴巴集团安全应急响应中心和 yycms。

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，天津市国瑞数码安全系统股份有限公司、北京天融信网络安全技术有限公司、北京启明星辰信息安全技术有限公司、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。奇安星城网络安全运营服务（长沙）有限公司、亚信科技（成都）有限公司、快页信息技术有限公司、联想集团、江苏金盾检测技术股份有限公司、内蒙古中叶信息技术有限责任公司、安徽锋刃信息科技有限公司、河南东方云盾信息技术有限公司、湖南泛联新安信息科技有限公司、内蒙古洞明科技有限公司、星云博创科技有限公司、河南灵创电子科技有限公司、上海直画科技有限公司、国网山东省电力公司、合肥梆梆信息科技有限公司、工业和信

息化部电子第五研究所、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、北京华顺信安信息技术有限公司、北京君云天下科技有限公司、比亚迪股份有限公司、北京微步在线科技有限公司、赛尔网络有限公司、贵州多彩网安科技有限公司、北京中关村实验室、江苏晟晖信息科技有限公司、中华人民共和国上海海事局、北京源堡科技有限公司、浙江木链物联网科技有限公司、河南悦海数安科技有限公司、四川中成基业安全技术有限公司、西藏熙安信息技术有限责任公司、中国邮政储蓄银行股份有限公司、广州安亿信软件科技有限公司、中孚安全技术有限公司、中国电信股份有限公司北京研究院、南京深安科技有限公司、山石网科通信技术股份有限公司、北京威努特技术有限公司、郑州埃文计算机科技有限公司、江苏金陵科技集团有限公司、苏州棱镜七彩信息科技有限公司及其他个人白帽子向 CNVD 提交了 23920 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、三六零数字安全科技集团有限公司和奇安信网神（补天平台）向 CNVD 共享的白帽子报送的 21126 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）	13187	13187
奇安信网神（补天平台）	7358	7358
天津市国瑞数码安全系统股份有限公司	2429	0
北京天融信网络安全技术有限公司	1294	24
北京启明星辰信息安全技术有限公司	899	12
北京神州绿盟科技有限公司	745	384
新华三技术有限公司	554	0
深信服科技股份有限公司	446	51
上海交大	381	381
北京数字观星科技有限公司	249	0
三六零数字安全科技集团有限公司	200	200
安天科技集团股份有限公司	180	0

阿里云计算有限公司	162	8
北京知道创宇信息技术有限公司	142	0
杭州安恒信息技术股份有限公司	130	31
京东科技信息技术有限公司	87	51
北京长亭科技有限公司	34	2
杭州迪普科技股份有限公司	21	0
远江盛邦（北京）网络安全科技股份有限公司	17	17
南京联成科技发展股份有限公司	13	13
中电科网络安全科技股份有限公司	7	7
贵州泰若数字科技有限公司	6	6
中国电信股份有限公司网络安全产品运营中心	6	6
西安四叶草信息技术有限公司	4	4
北京智游网安科技有限公司	2	2
北京信联数安科技有限公司	1	1
奇安星城网络安全运营服务（长沙）有限公司	98	98
亚信科技（成都）有限公司	63	63
快页信息技术有限公	55	55

司		
联想集团	46	46
江苏金盾检测技术股份有限公司	40	40
内蒙古中叶信息技术有限责任公司	38	38
安徽锋刃信息科技有限公司	30	30
河南东方云盾信息技术有限公司	25	25
湖南泛联新安信息科技有限公司	19	19
内蒙古洞明科技有限公司	14	14
星云博创科技有限公司	9	9
河南灵创电子科技有限公司	8	8
上海直画科技有限公司	7	7
国网山东省电力公司	5	5
合肥梆梆信息科技有限公司	4	4
工业和信息化部电子第五研究所	4	4
山东云天安全技术有限公司	4	4
北京山石网科信息技术有限公司	4	4
北京华顺信安信息技术有限公司	3	3
北京君云天下科技有限公司	3	3
比亚迪股份有限公司	3	3
北京微步在线科技有	3	3

限公司		
赛尔网络有限公司	3	3
贵州多彩网安科技有限公司	3	3
北京中关村实验室	3	3
江苏晟晖信息科技有限公司	3	3
中华人民共和国上海海事局	2	2
北京源堡科技有限公司	2	2
浙江木链物联网科技有限公司	2	2
河南悦海数安科技有限公司	2	2
四川中成基业安全技术有限公司	1	1
西藏熙安信息技术有限责任公司	1	1
中国邮政储蓄银行股份有限公司	1	1
广州安亿信软件科技有限公司	1	1
中孚安全技术有限公司	1	1
中国电信股份有限公司北京研究院	1	1
南京深安科技有限公司	1	1
山石网科通信技术股份有限公司	1	1
北京威努特技术有限公司	1	1
郑州埃文计算机科技有限公司	1	1

江苏金陵科技集团有限公司	1	1
苏州棱镜七彩信息科技有限公司	1	1
CNCERT 广西分中心	3	3
CNCERT 贵州分中心	1	1
个人	1654	1654
报送总计	30729	23920

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 204 个，应用程序 78 个，网络设备（交换机、路由器等网络端设备）32 个，智能设备（物联网终端设备）13 个，操作系统 12 个，数据库 7 个，安全产品 6 个，车联网 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	204
应用程序	78
网络设备（交换机、路由器等网络端设备）	32
智能设备（物联网终端设备）	13
操作系统	12
数据库	7
安全产品	6
车联网	1

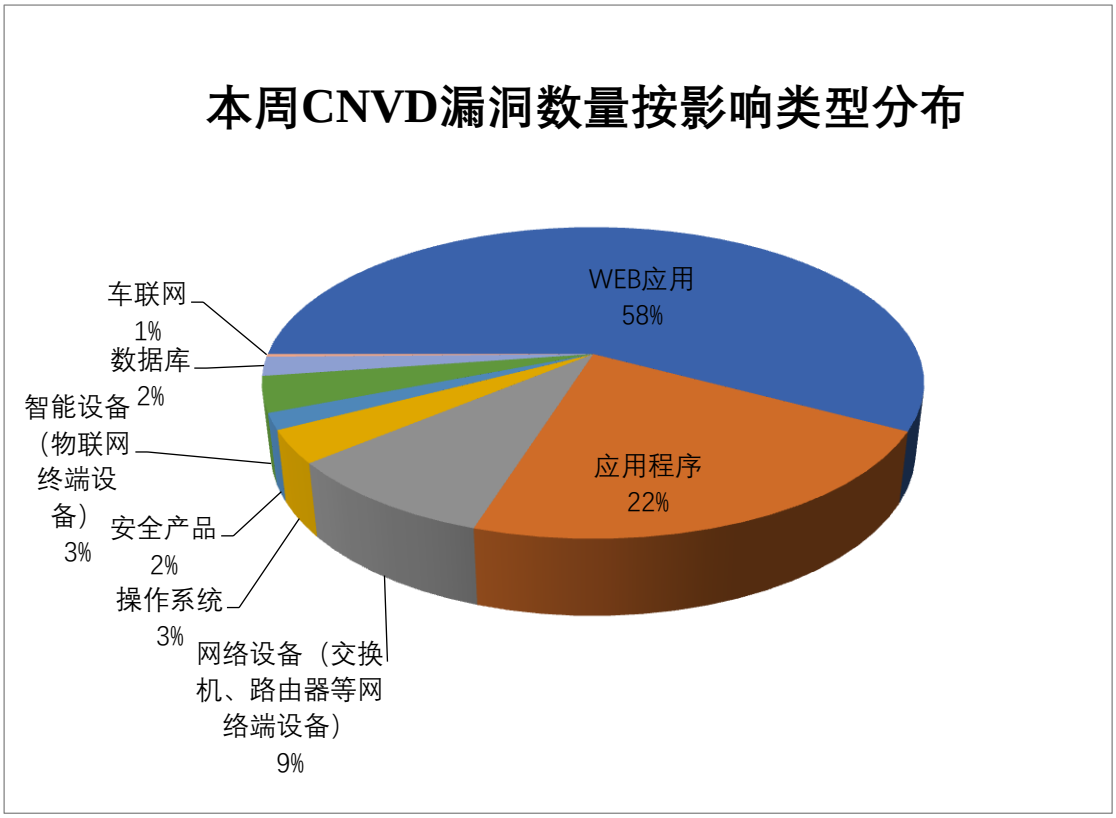

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及用友网络科技股份有限公司、IBM、WordPress 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	用友网络科技股份有限公司	14	4%
2	IBM	11	3%
3	WordPress	10	3%
4	Google	10	3%
5	Microsoft	10	3%
6	HCL Technologies	10	3%
7	北京百卓网络技术有限公司	8	2%
8	友讯电子设备（上海）有限公司	7	2%
9	北京星网锐捷网络技术有限公司	6	2%
10	其他	267	75%

本周行业漏洞收录情况

本周，CNVD 收录了 25 个电信行业漏洞，53 个移动互联网行业漏洞，3 个工控行业漏洞（如下图所示）。其中，“Huawei HarmonyOS 和 EMUI 授权问题漏洞、Siemens Tecnomatix Plant Simulation 越界写入漏洞（CNVD-2023-85374）”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/

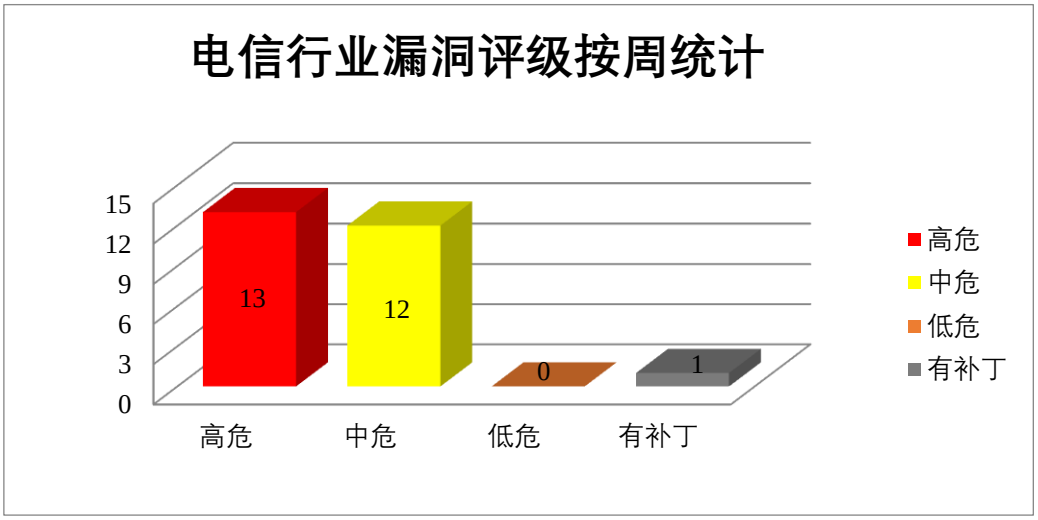

图 3 电信行业漏洞统计

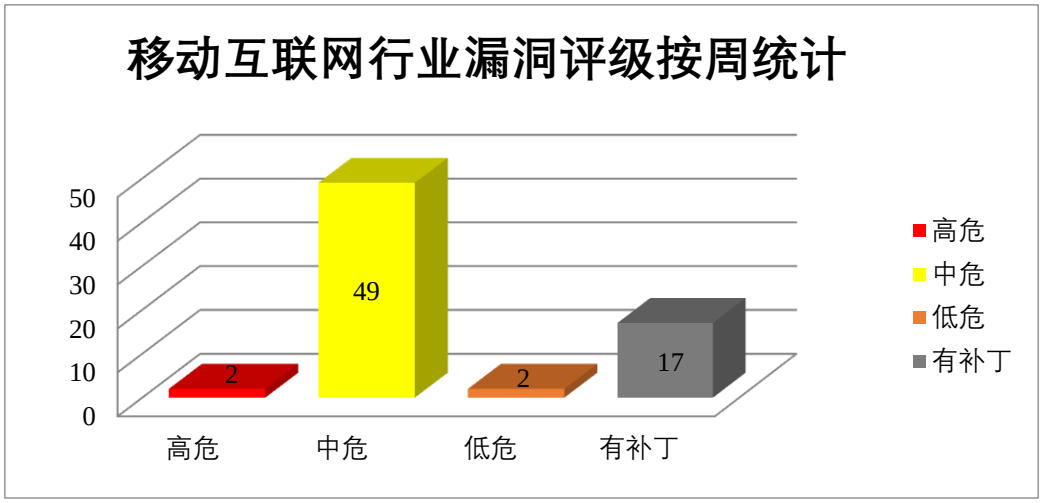

图 4 移动互联网行业漏洞统计

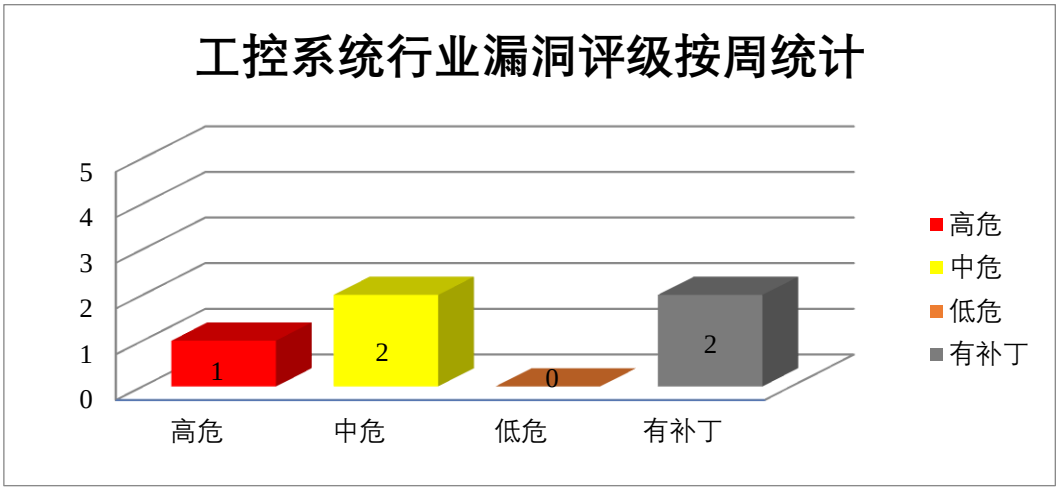

图 5 工控系统行业漏洞统计

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。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本地权限提升。

CNVD 收录的相关漏洞包括：Google Android 权限提升漏洞（CNVD-2023-84088、CNVD-2023-84087、CNVD-2023-84086、CNVD-2023-84089、CNVD-2023-84092、CNVD-2023-84091、CNVD-2023-84095、CNVD-2023-84094）。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-2023-84088
https://www.cnvd.org.cn/flaw/show/CNVD-2023-84087
https://www.cnvd.org.cn/flaw/show/CNVD-2023-84086
https://www.cnvd.org.cn/flaw/show/CNVD-2023-84089
https://www.cnvd.org.cn/flaw/show/CNVD-2023-84092
https://www.cnvd.org.cn/flaw/show/CNVD-2023-84091
https://www.cnvd.org.cn/flaw/show/CNVD-2023-84095
https://www.cnvd.org.cn/flaw/show/CNVD-2023-84094

2、 IBM 产品安全漏洞

IBM WebSphere Application Server Liberty 是美国国际商业机器（IBM）公司的一款构建于 Open Liberty 项目之上的 Java 应用程序服务器。IBM QRadar SIEM 是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 Security Verify Privilege

Manager 是一个用于公司环境中用于端点特权管理和应用程序控制的安全管理软件。该软件通过从端点移除本地管理权限，阻止恶意软件和勒索软件的无意下载进而攻击应用程序，利用 IBM Security Privilege Manager，可立即轻松执行最小特权和应用程序控制。IBM Security Verify Governance 是一个身份和访问管理解决方案。它是一种用于管理和监控用户身份、权限和访问的软件系统。IBM Sterling Partner Engagement Manager 是一个自动化管理工具。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞获取敏感信息，通过发送特制请求在系统上执行任意命令等。

CNVD 收录的相关漏洞包括：IBM WebSphere Application Server Liberty 资源管理错误漏洞、IBM QRadar SIEM 信息泄露漏洞（CNVD-2023-83656）、IBM Security Verify Privilege Manager 访问控制错误漏洞、IBM Security Verify Privilege Manager 任意文件上传漏洞、IBM Security Verify Governance 跨站脚本漏洞、IBM Security Verify Governance 硬编码漏洞（CNVD-2023-83661）、IBM Security Verify Governance 命令执行漏洞、IBM Sterling Partner Engagement Manager 身份验证错误漏洞。其中，“IBM WebSphere Application Server Liberty 资源管理错误漏洞、IBM Sterling Partner Engagement Manager 身份验证错误漏洞、IBM Security Verify Governance 命令执行漏洞、IBM Security Verify Privilege Manager 任意文件上传漏洞”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-2023-83658
https://www.cnvd.org.cn/flaw/show/CNVD-2023-83656
https://www.cnvd.org.cn/flaw/show/CNVD-2023-83664
https://www.cnvd.org.cn/flaw/show/CNVD-2023-83663
https://www.cnvd.org.cn/flaw/show/CNVD-2023-83662
https://www.cnvd.org.cn/flaw/show/CNVD-2023-83661
https://www.cnvd.org.cn/flaw/show/CNVD-2023-83660
https://www.cnvd.org.cn/flaw/show/CNVD-2023-83665

3、Microsoft 产品安全漏洞

Microsoft Message Queuing 是用于实现需要高性能的异步和同步场景的解决方案。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞在系统上执行任意代码，导致系统拒绝服务。

CNVD 收录的相关漏洞包括：Microsoft Message Queuing 拒绝服务漏洞（CNVD-2023-84123、CNVD-2023-84125、CNVD-2023-84124）、Microsoft Message Queuing 远程代码执行漏洞（CNVD-2023-84126、CNVD-2023-84127、CNVD-2023-84129、CNVD-2023-84128、CNVD-2023-84132）。其中，“Microsoft Message Queuing 拒绝服务漏洞（CNVD-2023-84123、CNVD-2023-84125、CNVD-2023-84124）”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-2023-84123
https://www.cnvd.org.cn/flaw/show/CNVD-2023-84126
https://www.cnvd.org.cn/flaw/show/CNVD-2023-84125
https://www.cnvd.org.cn/flaw/show/CNVD-2023-84124
https://www.cnvd.org.cn/flaw/show/CNVD-2023-84127
https://www.cnvd.org.cn/flaw/show/CNVD-2023-84129
https://www.cnvd.org.cn/flaw/show/CNVD-2023-84128
https://www.cnvd.org.cn/flaw/show/CNVD-2023-84132

4、HCL Technologies 产品安全漏洞

HCL Technologies Commerce 是美国 HCL Technologies 公司的一款用于电子商务的软件平台框架。该软件在可定制的集成软件包中包括营销，销售，客户和订单处理功能。HCL Technologies AppScan Presence 是一套动态分析测试工具，它主要用于 Web 安全测试。HCL Technologies BigFix Mobile 是一款移动设备管理（Mobile Device Management，MDM）解决方案。它旨在帮助企业和组织有效地管理和保护移动设备，包括智能手机、平板电脑和其他移动设备。HCL Technologies Traveler Companion 是一款 ios Iphone 和 Ipad 应用程序。用于在 Apple 设备上阅读加密的 Hcl Notes 邮件。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞获取敏感信息，使用特制的 URL 读取系统上的任意文件，获得提升的权限，上传恶意脚本，在系统上执行任意 PHP 代码等。

CNVD 收录的相关漏洞包括：HCL Technologies Commerce 目录遍历漏洞、HCL Technologies AppScan Presence 权限提升漏洞、HCL Technologies Compass 访问控制错误漏洞、HCL Technologies Compass 弱密码漏洞、HCL Technologies Compass 文件上传漏洞、HCL Technologies BigFix Mobile 跨站脚本漏洞、HCL Technologies BigFix Mobile 命令注入漏洞、HCL Technologies Traveler Companion 信息泄露漏洞。其中，“HCL Technologies Compass 访问控制错误漏洞、HCL Technologies Compass 弱密码漏洞、HCL Technologies Compass 文件上传漏洞、HCL Technologies BigFix Mobile 命令注入漏洞”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-2023-84324
https://www.cnvd.org.cn/flaw/show/CNVD-2023-84325
https://www.cnvd.org.cn/flaw/show/CNVD-2023-84326
https://www.cnvd.org.cn/flaw/show/CNVD-2023-84327
https://www.cnvd.org.cn/flaw/show/CNVD-2023-84328

https://www.cnvd.org.cn/flaw/show/CNVD-2023-84330

https://www.cnvd.org.cn/flaw/show/CNVD-2023-84331

https://www.cnvd.org.cn/flaw/show/CNVD-2023-84332

5、Zoo Management System 跨站脚本漏洞（CNVD-2023-85427）

Zoo Management System 是一个动物园管理系统。为动物园企业提供了一个在线和自动化平台来管理他们的日常记录。本周，Zoo Management System 被披露存在跨站脚本漏洞。攻击者可利用该漏洞通过注入精心设计的有效载荷执行任意 Web 脚本或 HTML。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-2023-85427

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

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-2023-83658	IBM WebSphere Application Server Liberty 资源管理错误漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.ibm.com/support/pages/node/7058356
CNVD-2023-83660	IBM Security Verify Governance 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://www.ibm.com/support/pages/node/7057377
CNVD-2023-83665	IBM Security Verify Privilege Manager 任意文件上传漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.ibm.com/support/pages/node/7047202
CNVD-2023-84123	Microsoft Message Queuing 拒绝服务漏洞（CNVD-2023-84123）	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-2023-36581
CNVD-2023-84124	Microsoft Message Queuing 拒绝服务漏洞（CNVD-2023-84124）	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-2023-36431
CNVD-2023-84323	Huawei HarmonyOS 和 EMUI 授权问题漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://consumer.huawei.com/cn/support/bulletin/2023/10/
CNVD-2023-84326	HCL Technologies Compass 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://support.hcltechsw.com/csm?id

			=kb_article&sysparm_article=KB0107511
CNVD-2023-84328	HCL Technologies Compass 文件上传漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0107510
CNVD-2023-84331	HCL Technologies BigFix Mobile 命令注入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0106372
CNVD-2023-85374	Siemens Tecnomatix Plant Simulation 越界写入漏洞（CNVD-2023-85374）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://cert-portal.siemens.com/productcert/pdf/ssa-764801.pdf

小结：本周，Google 产品被披露存在多个漏洞，攻击者可利用漏洞导致本地权限提升。此外，IBM、Microsoft、HCL Technologies 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，使用特制的 URL 读取系统上的任意文件，获得提升的权限，通过发送特制请求在系统上执行任意命令等。另外，Zoo Management System 被披露存在跨站脚本漏洞。攻击者可利用漏洞通过注入精心设计的有效载荷执行任意 Web 脚本或 HTML。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、D-Link DAR-7000 mailrecvview.php 文件 SQL 注入漏洞

验证描述

D-Link DAR-7000 是中国友讯（D-Link）公司的一款上网行为审计网关。

D-Link DAR-7000 mailrecvview.php 文件存在 SQL 注入漏洞，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/llixixi/cve/blob/main/D-LINK-DAR-7000_rce_%20mailrecvview.md

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2023-85604

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. SysAid IT 曝出零日漏洞，需尽快安装补丁

为了更大程度的降低勒索软件攻击的伤害，使用 SysAid 的企业最好尽快安装补丁。同时要注意在打补丁之前扫描环境，看看是否有被利用的迹象。

参考链接：https://www.freebuf.com/news/383432.html

2. SUMO LOGIC 披露了安全漏洞，并建议客户更换凭据

Sumo Logic 是一家网络安全公司，专门从事基于云的日志管理和分析。该公司在上周发现其 AWS 账户遭到入侵后披露了安全漏洞。

参考链接：https://securityaffairs.com/153882/security/sumo-logic-security-breach.html?_gl=1*ef53jz*_ga*MTQ2MTcwNDA4Ni4xNjY2NzcyNzE4*_ga_NPN4VEKBTY*MTY5OTUyMzAwNy4yOTAuMC4xNjk5NTIzMDA3LjYwLjAuMA..*_ga_8ZWTX5HC4Z*MTY5OTUyMzAxMS4xNjEuMC4xNjk5NTIzMDExLjAuMC4w&_ga=2.5556

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