国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2022 年 12 月 5 日-2022 年 12 月 11 日 **2022 年第 49 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 600 个，其中高危漏洞 259 个、中危漏洞 297 个、低危漏洞 44 个。漏洞平均分值为 6.41。本周收录的漏洞中，涉及 0day 漏洞 347 个（占 58%），其中互联网上出现“WAVLINK WN531G3 访问控制错误漏洞、Linux kernel 内存错误引用漏洞”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 5742 个，与上周（16272 个）环比减少 65%。

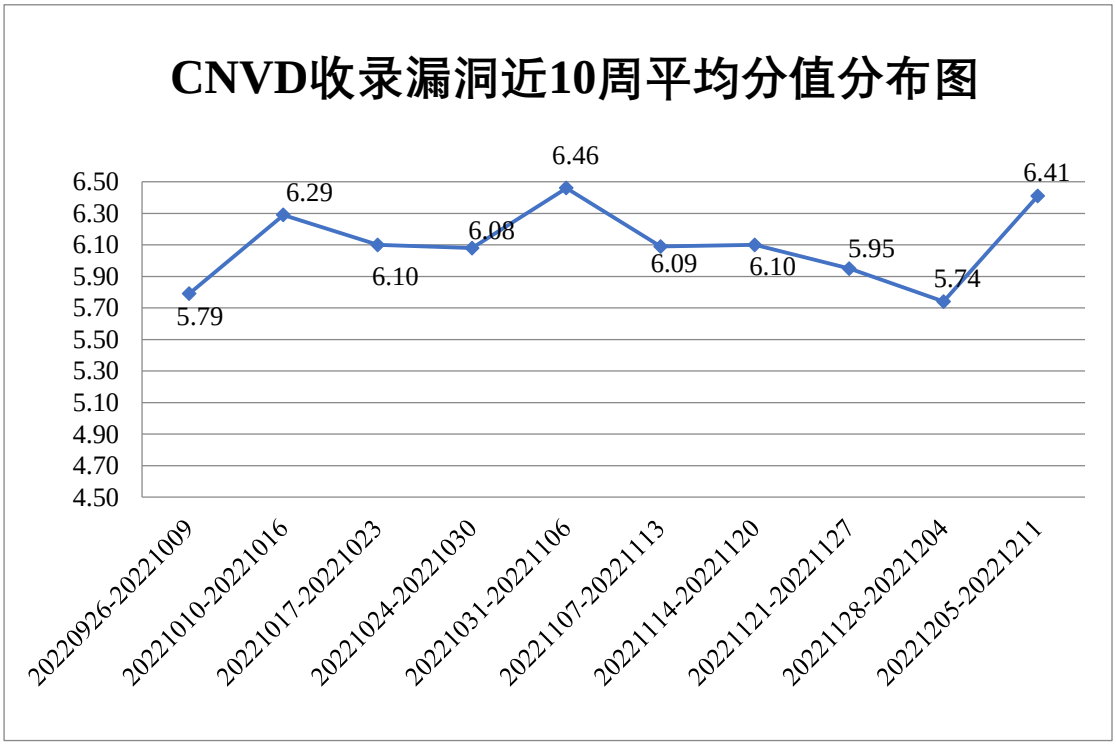

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 51 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 758 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 128 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、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、郑州领浩电子科技有限公司、浙江宇视科技有限公司、浙江兰德纵横网络技术股份有限公司、浙江和达科技股份有限公司、浙江大华技术股份有限公司、友讯电子设备（上海）有限公司、用友网络科技股份有限公司、一城一家网络科技有限公司、兄弟（中国）商业有限公司、夏普科技（上海）有限公司、西安众邦网络科技有限公司、武汉儒松科技有限公司、通用电气（中国）有限公司、台达集团、苏州市轨道交通集团有限公司、苏州开心盒子软件有限公司、苏州汇川技术有限公司、水月居科技有限公司、世邦通信股份有限公司、深圳智慧光迅信息技术有限公司、深圳维盟科技股份有限公司、深圳市中科网威科技有限公司、深圳市智岩科技有限公司、深圳市网域科技技术有限公司、深圳市网心科技有限公司、深圳市四海众联网络科技有限公司、深圳市思迅软件股份有限公司、深圳市慎勇科技有限公司、深圳市乔安科技有限公司、深圳市吉祥腾达科技有限公司、深圳市河辰通讯技术有限公司、深圳市超脑云信息技术有限公司、深圳绿米联创科技有限公司、深圳彼度科技有限公司、上海紫灏信息技术有限公司、上海挚达科技发展股份有限公司、上海展盟网络科技有限公司、上海熙软科技有限公司、上海茸易科技有限公司、上海金电网安科技有限公司、上海孚盟软件有限公司、上海泛微网络科技股份有限公司、上海博达数据通信有限公司、上海贝锐信息科技股份有限公司、上海北辰软件股份有限公司、上海阿法迪智能数字科技股份有限公司、厦门四信通信科技有限公司、厦门美易通软件科技有限公司、厦门爱陆通通信科技有限公司、三盟科技股份有限公司、睿易教育科技股份有限公司、瑞斯康达科技发展股份有限公司、青岛易软天创网络科技有限公司、青岛东胜伟业软件有限公司、青岛爱米云软件有限公司、普联技术有限公司、南京帆软软件有限公司、联奕科技股份有限公司、金蝶天燕云计算股份有限公司、江西铭软科技有限公司、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、基恩士（中国）有限公司、慧星软件科技有限公司、惠普贸易（上海）有限公司、河北天海网络工程有限公司、杭州雄伟科技开发股份有限公司、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、杭州博采网络科技股份有限公司、国泰恒安建设集团有限公司、桂林零与壹软件有限公司、桂林佳朋信息科技有限公司、桂林崇胜网络科技有限公司、广州同聚成电子科技有限公司、广州市九安物联科技有限公司、广州烈驹电子科技有限公司、广联达科技股份有限公司、帆软

软件有限公司、东莞誉云网络科技有限公司、大唐电信科技股份有限公司、驰宇科技有限公司、成都卓越远扬信息技术有限公司、成都零起飞科技有限公司、成都华迈通信技术有限公司、成都飞鱼星科技股份有限公司、畅捷通信息技术股份有限公司、北京中远麒麟科技有限公司、北京中成科信科技发展有限公司、北京智慧远景科技产业股份有限公司、北京星网锐捷网络技术有限公司、北京文网亿联科技有限公司、北京网康科技有限公司、北京万户网络技术有限公司、北京通达信科科技有限公司、北京世纪超星信息技术发展有限责任公司、北京趋势威尔网络技术有限公司、北京派网软件有限公司、北京龙软科技股份有限公司、北京朗新天霁软件技术有限公司、北京库巴扎信息科技有限公司、北京金和网络股份有限公司、北京华富远科技术有限公司、北京宏景世纪软件股份有限公司、北京国炬信息技术有限公司、北京碧海威科技有限公司、北京百卓网络技术有限公司、安美世纪（北京）科技有限公司、阿里巴巴集团安全应急响应中心、ZyXEL、PESCMS 和《中国学术期刊（光盘版）》电子杂志社有限公司。

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，新华三技术有限公司、深信服科技股份有限公司、安天科技集团股份有限公司、西安四叶草信息技术有限公司、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。杭州默安科技有限公司、奇安星城网络安全运营服务（长沙）有限公司、北京山石网科信息技术有限公司、重庆都会信息科技有限公司、博智安全科技股份有限公司、浙江木链物联网科技有限公司、中国工商银行股份有限公司软件开发中心、杭州海康威视数字技术股份有限公司、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、苏州棱镜七彩信息科技有限公司、重庆易阅科技有限公司、贵州多彩网安科技有限公司、星云博创科技有限公司、河南灵创电子科技有限公司、上海谋乐网络科技有限公司、北京云科安信科技有限公司（Seraph 安全实验室）、赛尔网络有限公司、山东九域信息技术有限公司、广东唯顶信息科技股份有限公司、福建省海峡信息技术有限公司、河南悦海数安科技有限公司、快页信息技术有限公司、上海纽盾科技股份有限公司、江苏易安联网络技术有限公司、苏州亿阳值通科技发展股份有限公司、北京安帝科技有限公司、山石网科通信技术股份有限公司、浙江信安昆仑信息技术有限公司、中通服创发科技有限责任公司、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、郑州埃文科技、安徽信科共创信息安全测评有限公司、北京微步在线科技有限公司、北京冠程科技有限公司、福州启云信息技术有限公司、杭州美创科技有限公司、麒麟软件有限公司、广州安亿信软件科技有限公司、北京瑾逸海阔科技有限公司、北京万户网络技术有限公司、中国—东盟信息港股份有限公司、河北千诚电子科技有限公司、黄河勘测规划设计研究院有限公司、中国电信股份有限公司网络安全产品运营中心及及其他个人白帽子向 CNVD 提交了 5742 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）、三六零数字安全科技集团有限公司、奇安信网神（补天平台）、上海交大和向 CNVD 共享的白帽子报送的 3232 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）	1265	1265
三六零数字安全科技集团有限公司	918	918
奇安信网神（补天平台）	560	560
上海交大	489	489
新华三技术有限公司	409	1
深信服科技股份有限公司	370	0
安天科技集团股份有限公司	314	1
西安四叶草信息技术有限公司	269	269
北京神州绿盟科技有限公司	189	6
北京启明星辰信息安全技术有限公司	154	15
北京天融信网络安全技术有限公司	137	8
远江盛邦（北京）网络安全科技股份有限公司	116	116
恒安嘉新（北京）科技股份公司	105	1
北京数字观星科技有限公司	105	0
杭州安恒信息技术股份有限公司	79	19
卫士通信息产业股份有限公司	69	69
内蒙古云科数据服务	35	35

股份有限公司		
中国电信集团系统集成有限责任公司	29	0
北京知道创宇信息技术有限公司	28	1
南京众智维信息科技有限公司	22	22
深圳市腾讯计算机系统有限公司（玄武实验室）	21	21
京东科技信息技术有限公司	8	0
北京华顺信安信息技术有限公司	6	6
杭州迪普科技股份有限公司	3	3
杭州默安科技有限公司	177	177
奇安星城网络安全运营服务（长沙）有限公司	140	140
北京山石网科信息技术有限公司	34	34
重庆都会信息科技有限公司	31	31
博智安全科技股份有限公司	30	30
浙江木链物联网科技有限公司	28	28
中国工商银行股份有限公司软件开发中心	23	23
杭州海康威视数字技术股份有限公司	22	22
安徽锋刃信息科技有限公司	20	20

河南东方云盾信息技术有限公司	20	20
苏州棱镜七彩信息科技有限公司	15	15
重庆易阅科技有限公司	14	14
贵州多彩网安科技有限公司	13	13
星云博创科技有限公司	11	11
河南灵创电子科技有限公司	10	10
上海谋乐网络科技有限公司	10	10
北京云科安信科技有限公司（Seraph 安全实验室）	9	9
赛尔网络有限公司	8	8
山东九域信息技术有限公司	7	7
广东唯顶信息科技股份有限公司	7	7
福建省海峡信息技术有限公司	5	5
河南悦海数安科技有限公司	5	5
快页信息技术有限公司	5	5
上海纽盾科技股份有限公司	5	5
江苏易安联网络技术有限公司	4	4
苏州亿阳值通科技发展股份有限公司	4	4
北京安帝科技有限公	4	4

司		
山石网科通信技术股份有限公司	4	4
浙江信安昆仑信息技术有限公司	3	3
中通服创发科技有限责任公司	2	2
长春嘉诚信息技术股份有限公司	2	2
山东新潮信息技术有限公司	2	2
郑州埃文科技	2	2
安徽信科共创信息安全测评有限公司	1	1
北京微步在线科技有限公司	1	1
北京冠程科技有限公司	1	1
福州启云信息技术有限公司	1	1
杭州美创科技有限公司	1	1
麒麟软件有限公司	1	1
广州安亿信软件科技有限公司	1	1
北京瑾逸海阔科技有限公司	1	1
北京万户网络技术有限公司	1	1
中国—东盟信息港股份有限公司	1	1
河北千诚电子科技有限公司	1	1
黄河勘测规划设计研究院有限公司	1	1

亚信科技（成都）有限公司	1	0
中国电信股份有限公司网络安全产品运营中心	1	1
CNCERT 四川分中心	3	3
CNCERT 贵州分中心	1	1
CNCERT 云南分中心	1	1
CNCERT 内蒙古分中心	1	1
个人	1222	1222
报送总计	7618	5742

本周漏洞按类型和厂商统计

本周，CNVD 收录了 600 个漏洞。WEB 应用 337 个，应用程序 138 个，网络设备（交换机、路由器等网络端设备）82 个，操作系统 17 个，智能设备（物联网终端设备）17 个，安全产品 5 个，数据库 4 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	337
应用程序	138
网络设备（交换机、路由器等网络端设备）	82
操作系统	17
智能设备（物联网终端设备）	17
安全产品	5
数据库	4

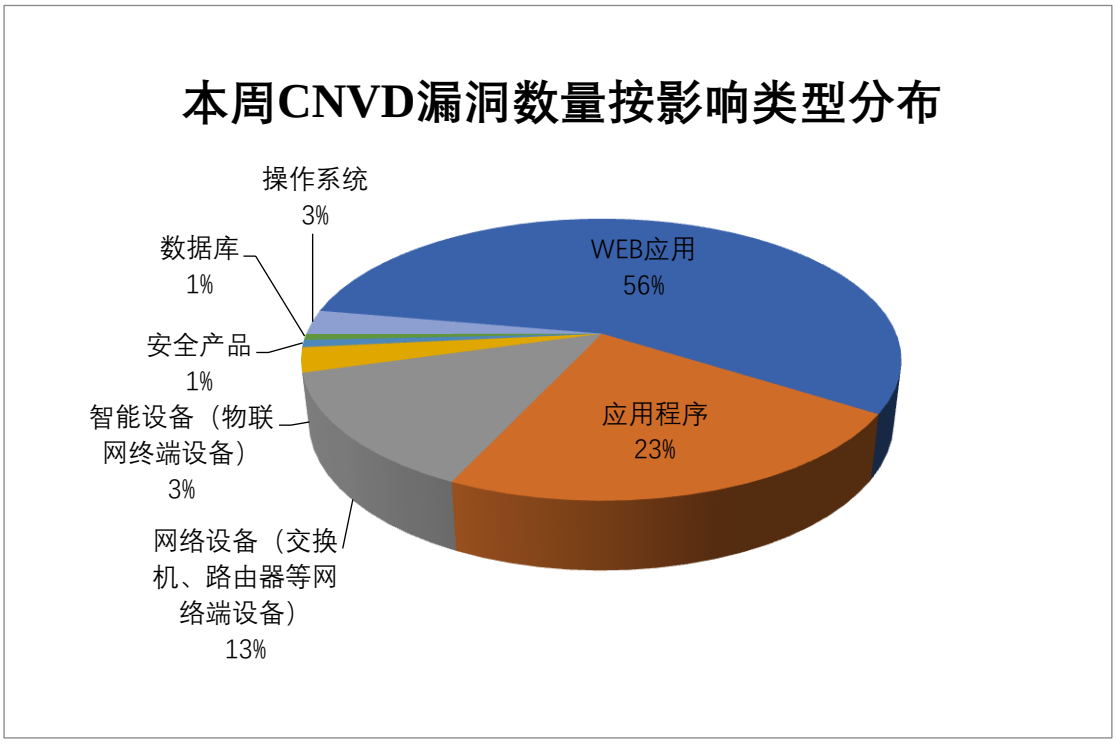

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞 WordPress、Dell、Google 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	49	8%
2	Dell	20	3%
3	Google	19	3%
4	IBM	11	2%
5	Microsoft	9	2%
6	新华三技术有限公司	11	2%
7	NETGEAR	7	1%
8	Samsung	7	1%
9	XWiki	7	1%
10	其他	460	77%

本周行业漏洞收录情况

本周，CNVD 收录了 45 个电信行业漏洞，28 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，“Mitsubishi Electric Corporation MELSEC iQ-R Series 输入验证错误漏洞、ABB MicroSCADA Pro SYS600 代码执行漏洞、Google Android 拒绝服务漏洞（CNVD-2022-85764）”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/

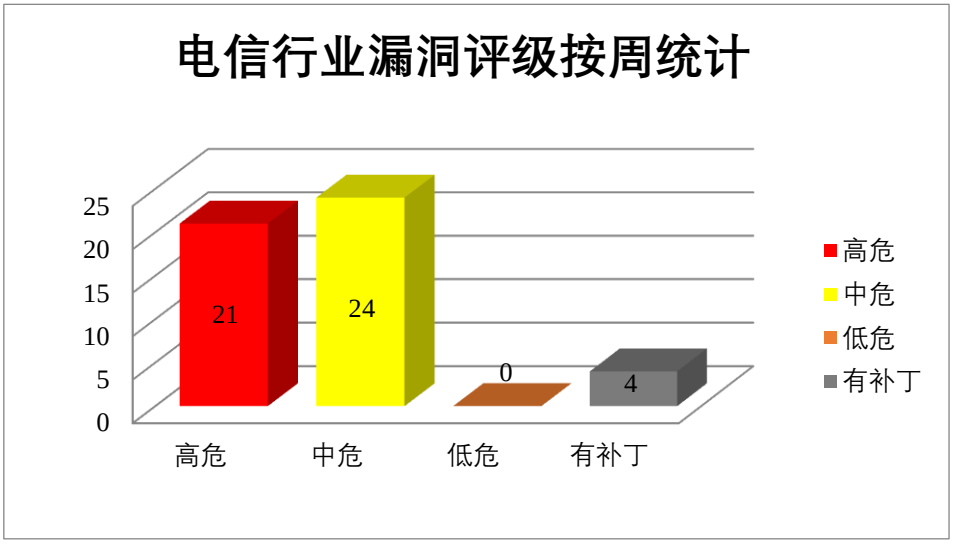

图 3 电信行业漏洞统计

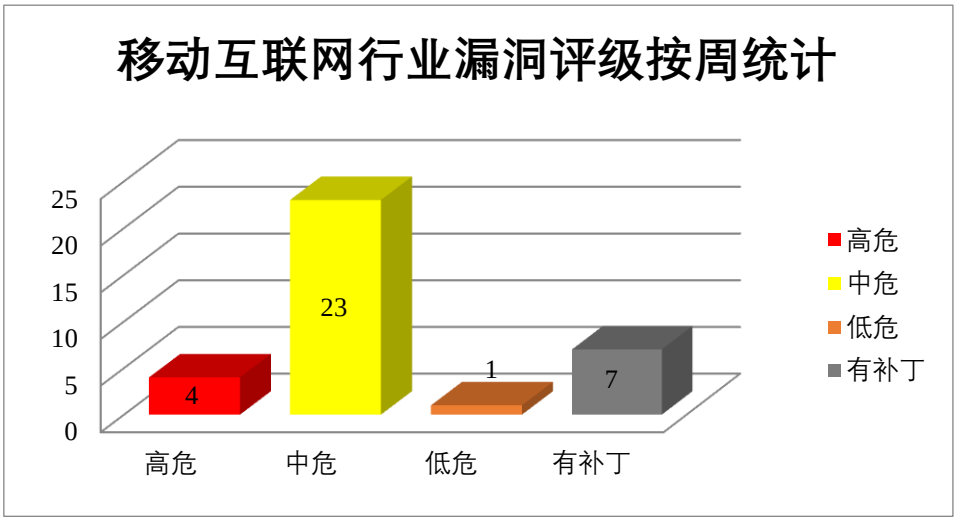

图 4 移动互联网行业漏洞统计

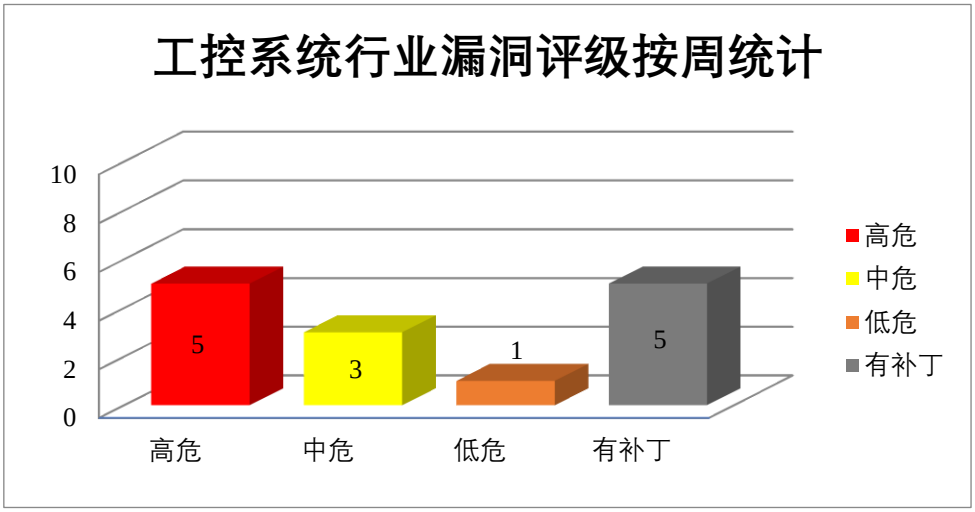

图 5 工控系统行业漏洞统计

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 Windows 是一套个人设备使用的操作系统。Microsoft Windows Server 是一套服务器操作系统。Windows Print Spooler 是其中的一个打印后台处理程序。Microsoft Windows DWM Core Library 是美国微软（Microsoft）公司的一个核心库。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞以更高的权限执行任意代码。

CNVD 收录的相关漏洞包括：Microsoft Windows DWM Core Library 权限提升漏洞（CNVD-2022-84603）、Microsoft Windows Print Spooler 权限提升漏洞（CNVD-2022-84604、CNVD-2022-84605）、Microsoft Windows DNS Server 远程代码执行漏洞（CNVD-2022-84606、CNVD-2022-84607、CNVD-2022-84608、CNVD-2022-84609、CNVD-2022-84610）。其中，除“Microsoft Windows DWM Core Library 权限提升漏洞（CNVD-2022-84603）、Microsoft Windows Print Spooler 权限提升漏洞（CNVD-2022-84604、CNVD-2022-84605）”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-2022-84603

https://www.cnvd.org.cn/flaw/show/CNVD-2022-84604

https://www.cnvd.org.cn/flaw/show/CNVD-2022-84605

https://www.cnvd.org.cn/flaw/show/CNVD-2022-84606

https://www.cnvd.org.cn/flaw/show/CNVD-2022-84607

https://www.cnvd.org.cn/flaw/show/CNVD-2022-84608

https://www.cnvd.org.cn/flaw/show/CNVD-2022-84609

https://www.cnvd.org.cn/flaw/show/CNVD-2022-84610

2、 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多个漏洞，攻击者可利用漏洞绕过安全限制，在系统上执行任意代码，或者导致应用程序崩溃。

CNVD 收录的相关漏洞包括：Google Chrome Extensions 代码执行漏洞、Google Chrome 安全绕过漏洞（CNVD-2022-85084）、Google Chrome Media Galleries 缓冲区溢出漏洞、Google Chrome Layout 代码执行漏洞、Google Chrome V8 代码执行漏洞（CNVD-2022-85088）、Google Chrome 安全绕过漏洞（CNVD-2022-85089）、Google Chrome Accessibility 代码执行漏洞、Google Chrome Feedback service 代码执行漏洞。上述漏洞的综合评级为“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-2022-85083

https://www.cnvd.org.cn/flaw/show/CNVD-2022-85084

https://www.cnvd.org.cn/flaw/show/CNVD-2022-85085

https://www.cnvd.org.cn/flaw/show/CNVD-2022-85086

https://www.cnvd.org.cn/flaw/show/CNVD-2022-85088

https://www.cnvd.org.cn/flaw/show/CNVD-2022-85089

https://www.cnvd.org.cn/flaw/show/CNVD-2022-85090

https://www.cnvd.org.cn/flaw/show/CNVD-2022-85091

3、 Dell 产品安全漏洞

Dell BSAFE Micro Edition Suite 是一个可为 c/c++应用、设备、系统提供加密、证书和传输层安全性的开发工具包。Dell BIOS 是美国戴尔（Dell）公司的一个计算机主板上小型内存芯片上的嵌入式软件。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞通过向 SMI 发送恶意输入来绕过在 SMM 中的安全控制，可执行任意代码，造成拒绝服务攻击等。

CNVD 收录的相关漏洞包括：Dell BSAFE Micro Edition Suite 缓冲区溢出漏洞（CNVD-2022-84622）、Dell BIOS 输入验证错误漏洞（CNVD-2022-85079、CNVD-2022-85078、CNVD-2022-85077、CNVD-2022-85076、CNVD-2022-85082、CNVD-2022-85081、CNVD-2022-85080）。其中，除“Dell BSAFE Micro Edition Suite 缓冲区溢出漏洞（CNVD-2022-84622）”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-2022-84622

https://www.cnvd.org.cn/flaw/show/CNVD-2022-85079

https://www.cnvd.org.cn/flaw/show/CNVD-2022-85078

https://www.cnvd.org.cn/flaw/show/CNVD-2022-85077

https://www.cnvd.org.cn/flaw/show/CNVD-2022-85076

https://www.cnvd.org.cn/flaw/show/CNVD-2022-85082

https://www.cnvd.org.cn/flaw/show/CNVD-2022-85081

https://www.cnvd.org.cn/flaw/show/CNVD-2022-85080

4、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 DB2 是美国国际商业机器（IBM）公司的一套关系型数据库管理系统。该系统的执行环境主要有 UNIX、Linux、IBMi、z/OS 以及 Windows 服务器版本。IBM AIX 是美国国际商业机器（IBM）公司的一款为 IBM Power 体系架构开发的一种基于开放标准的 UNIX 操作系统。IBM Sterling Partner Engagement Manager 是美国 IBM 公司的一个自动化管理工具。IBM UrbanCode Deploy（UCD）是美国 IBM 公司的一套应用自动化部署工具。该工具基于一个应用部署自动化管理信息模型，并通过远程代理技术，实现对复杂应用在不同环境下的自动化部署等。IBM OPENBMC 是美国国际商用机器公司（IBM）公司的一个模拟器。IBM InfoSphere Information Server 是美国国际商业机器（IBM）公司的一套数据整合平台。该平台可用于整合各种渠道获取的数据信息。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，发起拒绝服务攻击等。

CNVD 收录的相关漏洞包括：IBM WebSphere Application Server Liberty 拒绝服务漏洞、IBM Db2 信息泄露漏洞（CNVD-2022-85416）、IBM AIX 和 VIOS 权限提升漏洞、IBM DB2 跨站请求伪造漏洞、IBM Sterling Partner Engagement Manager XML 外部实体注入漏洞、IBM UrbanCode Deploy 信息泄露漏洞、IBM OPENBMC 拒绝服务漏洞、IBM InfoSphere Information Server 信息泄露漏洞（CNVD-2022-85418）。其中，“IBM DB2 跨站请求伪造漏洞、IBM Sterling Partner Engagement Manager XML 外部实体注入漏洞”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-2022-85327

https://www.cnvd.org.cn/flaw/show/CNVD-2022-85416

https://www.cnvd.org.cn/flaw/show/CNVD-2022-85415

https://www.cnvd.org.cn/flaw/show/CNVD-2022-85414

https://www.cnvd.org.cn/flaw/show/CNVD-2022-85421

https://www.cnvd.org.cn/flaw/show/CNVD-2022-85420

https://www.cnvd.org.cn/flaw/show/CNVD-2022-85419

https://www.cnvd.org.cn/flaw/show/CNVD-2022-85418

5、D-Link DIR-882 webGetVarString 函数缓冲区溢出漏洞

D-Link DIR-882 是中国友讯（D-Link）公司的一款无线路由器。本周，D-Link DIR-882 被披露存在缓冲区溢出漏洞。该漏洞源于其 webGetVarString 函数对输入数据缺乏长度验证，攻击者可利用漏洞导致拒绝服务或者远程代码执行。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-2022-85551

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-2022-85764	Google Android 拒绝服务漏洞（CNVD-2022-85764）	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/android-13
CNVD-2022-86324	Zyxel LTE3301-M209 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/global/en/support/security-advisories/zyxel-security-advisory-for-pre-configured-password-vulnerability-of-lte3301-m209
CNVD-2022-86327	NETGEAR R7000P wan_dns1_pri 缓冲区溢出漏洞	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.netgear.com/about/security/
CNVD-2022-86329	Schneider Electric 产品授权问题漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://www.se.com/us/en/download/document/SEVD-2022-102-02/
CNVD-2022-86331	ABB MicroSCADA Pro SYS600 代码执行漏洞	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.hitachienergy.com/
CNVD-2022-86350	Google Chrome 存在未明漏洞（CNVD-2022-86350）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://chromereleases.googleblog.com/2022/11/stable-channel-update-for-desktop_29.html
CNVD-2022-86371	WordPress WP Affiliate Platform plugin 跨站请求伪造漏洞	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.wordfence.com/vulnerab

			ility-advisories-continued/#CVE-2022-3898
CNVD-2022-86385	MOXA ARM-Based Computers 权限提升漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链：https://www.moxa.com/en/support/product-support/security-advisory/moxa-arm-based-computer-improper-privilege-management-vulnerability
CNVD-2022-86536	pgAdmin 4 远程代码执行漏洞	高	用户可联系供应商获得补丁信息：https://www.pgadmin.org/
CNVD-2022-86535	ThinkPHP 命令执行漏洞（CNVD-2022-86535）	高	用户可联系供应商获得补丁信息：https://www.thinkphp.cn/

小结：本周，Microsoft 产品被披露存在多个漏洞，攻击者可利用漏洞以更高的权限执行任意代码。此外，Google、Dell、IBM 等多款产品被披露存在多个漏洞，攻击者可利用漏洞绕过安全限制，获取敏感信息，在系统上执行任意代码，或者导致应用程序崩溃等。另外，D-Link DIR-882 被披露存在缓冲区溢出漏洞。攻击者可利用漏洞导致拒绝服务或者远程代码执行。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、WAVLINK WN531G3 访问控制错误漏洞

验证描述

WAVLINK WN531G3 是中国睿因科技（WAVLINK）公司的一个无线路由器。

WAVLINK WN531G3 M31G3.V5030.201204 版本和 M31G3.V5030.200325 版本存在访问控制错误漏洞，攻击者可利用该漏洞下载配置数据和日志文件。

验证信息

POC 链接：https://github.com/strik3r0x1/Vulns/blob/main/Wavlink%20WL-WN531G3.md

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2022-86355

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. AMI MegaRAC 漏洞影响 AMD、ARM、HPE、Dell 等众多服务器

Bleeping Computer 网站披露，Eclypsium 的研究人员发现美国 Megatrends MegaRAC 基板管理控制器（BMC）软件中存在三个漏洞，这些漏洞影响许多云服务和数据中心运营商使用的服务器设备。

参考链接：https://www.freebuf.com/news/351686.html

2. 三菱电机 PLC 曝出多个安全漏洞

美国网络安全和基础设施安全局 (CISA) 在上周发布了一份工业控制系统 (ICS) 咨询，对三菱电机 GX Works3 工程软件存在的多个漏洞发出了安全警告。在 CISA 揭露的 10 个缺陷中，有 3 个涉及敏感数据的明文存储，4 个涉及使用硬编码加密密钥，2 个涉及使用硬编码密码，1 个涉及凭证保护不足。CVE-2022-25164 和 CVE-2022-29830 的 CVSS 评分高达 9.1，可在无需任何权限的情况下被滥用，以获取对 CPU 模块的访问权限并获取有关项目文件的信息。

参考链接：https://www.freebuf.com/news/351595.html

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