国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2023 年 08 月 28 日-2023 年 09 月 03 日　　2023 年第 35 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 337 个，其中高危漏洞 130 个、中危漏洞 186 个、低危漏洞 21 个。漏洞平均分值为 6.58。本周收录的漏洞中，涉及 0day 漏洞 212 个（占 63%），其中互联网上出现“Badaso 跨站脚本漏洞、Bento4 拒绝服务漏洞（CNVD-2023-66174）”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 13976 个，与上周（17404 个）环比减少 20%。

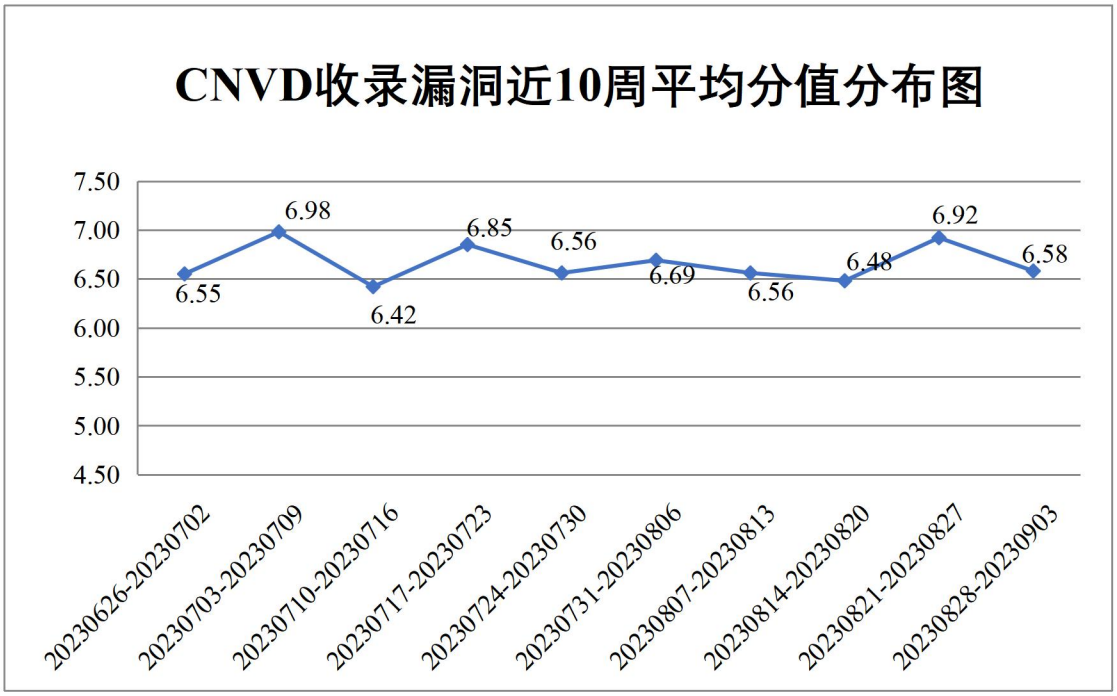

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 28 起，向基础电

信企业通报漏洞事件 7 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 820 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 131 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 41 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：

淄博闪灵网络科技有限公司、珠海金山办公软件有限公司、重庆葆慷优品电子商务有限公司、中興保全科技、中天城投集团物业管理有限公司、中农国华农业科技（北京）有限公司、中旅国际会议展览有限公司、中科同昌信息技术集团有限公司、中国对外经济贸易信托有限公司、中标软件有限公司、之寓置业有限公司、浙江兰德纵横网络技术股份有限公司、浙江寰福科技有限公司、浙江标点信息科技有限公司、云大夫网络科技（苏州）有限公司、袁志蒙工作室、友讯电子设备（上海）有限公司、用友网络科技股份有限公司、一掌控（上海）互联网科技有限公司、一诺（鞍山）信息科技有限责任公司、西安瑞友信息技术资讯有限公司、武汉同富通商贸有限公司、武汉天际航信息科技股份有限公司、武汉圣合软件技术有限公司、万兴科技集团股份有限公司、天津天堰科技股份有限公司、天津上医互联网医院有限公司、腾讯安全应急响应中心、淘惠（佛山）网络科技有限公司、太原时空超越科技有限公司、苏州赏聘网络科技有限公司、四川易泊时捷智能科技有限公司、四川迅睿云软件开发有限公司、十三曜（厦门）大数据科技有限公司、圣旦（北京）文化传媒有限公司、深圳致软信息技术有限公司、深圳云鹿信息科技有限公司、深圳市云顶信息技术有限公司、深圳市亿图软件有限公司、深圳市雄帝科技股份有限公司、深圳市网心科技有限公司、深圳市拓普泰尔科技有限公司、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、深圳市宏拓新软件有限公司、深圳市和为顺网络技术有限公司、深圳市昂捷信息技术股份有限公司、深信服科技股份有限公司、申瓯通信设备有限公司、上海英立视数字科技有限公司、上海荃路软件开发工作室、上海力软信息技术有限公司、上海肯特仪表股份有限公司、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、上海测吧信息技术有限公司、上海布雷德科技有限公司、上海必智科技有限公司、上海傲卓教育科技有限公司、山西供销农芯乐电子商务有限公司、山东云时空信息科技有限公司、山东山大华天软件有限公司、山东千乘优品电子商务有限公司、山东力创科技股份有限公司、山东科德电子有限公司、山东金钟科技集团股份有限公司、山东金麦数字技术有限公司、厦门昕桐科技有限公司、森思达能源技术服务有限公司、任子行网络技术股份有限公司、青岛锐商软件开发有限公司、青岛全卫肿瘤互联网医院有限公司、青岛海威茨仪表有限公司、青岛海石商用科技股份有限公司、普联技术有限公司、鹏为软件股份有限公司、南阳宏恩科技有限公司、南通云尚找家纺电子商务有限公司、南京博纳睿通软件科技有限公司、秒优大数据科技（杭州）有限公司、美林数据技术股份有限公司、蚂蚁科技集

团股份有限公司、罗克韦尔自动化（中国）有限公司、凌霞（深圳）软件有限公司、浪潮电子信息产业股份有限公司、昆明奥远科技有限公司、科大讯飞信息科技股份有限公司、京迈（湖北）电子商务股份有限公司、金卡银证软件（杭州）有限公司、江苏中天互联科技有限公司、江苏汇文软件有限公司、佳能（中国）有限公司、济宁云课网络科技有限公司、吉翁电子（深圳）有限公司、淮南市银泰软件科技有限公司、湖南传递幸福科技有限公司、河北赢图网络科技有限公司、合肥优品信息服务有限公司、合肥盛东信息科技有限公司、好嗨油能源科技（河南）有限公司、杭州圆图网络技术有限公司、杭州雄伟科技开发股份有限公司、杭州新中大科技股份有限公司、杭州图南电子股份有限公司、杭州汇点网络科技有限公司、杭州海康威视数字技术股份有限公司、广州思迈特软件有限公司、广州德生智能信息技术有限公司、广西朗杰智慧科技发展有限公司、广西聚养优品电子商务有限公司、广联达科技股份有限公司、馥鸿科技股份有限公司、福建顶点软件股份有限公司、飞塔信息科技(北京)有限公司、鼎捷软件股份有限公司、郸城县新翔软件科技有限公司、大连富豪科技有限公司、大连栋科软件工程有限公司、齿象无形（深圳）咨询有限公司、成都网旗云科信息技术有限公司、成都德芯数字科技股份有限公司、畅捷通信息技术股份有限公司、常州普盛力紧固件有限公司、北京中农信达信息技术有限公司、北京智齿博创科技有限公司、北京致远互联软件股份有限公司、北京亿赛通科技发展有限责任公司、北京讯易智科技发展有限公司、北京星网锐捷网络技术有限公司、北京香哈网络股份有限公司、北京网康科技有限公司、北京网达立信信息技术有限公司、北京万户软件技术有限公司、北京完美创意科技有限公司、北京通达信科科技有限公司、北京泰尔赛科科技有限公司、北京寺库商贸有限公司、北京润乾信息系统技术有限公司、北京润尼尔科技股份有限公司、北京巧巧时代网络科技有限公司、北京启明星辰信息安全技术有限公司、北京欧倍尔软件技术开发有限公司、北京喵山汪海科技有限公司、北京朗新天霁软件技术有限公司、北京久其软件股份有限公司、北京九思协同软件有限公司、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、百度安全应急响应中心、安美世纪（北京）科技有限公司、安徽幸福快送网络科技有限公司、安徽江淮汽车集团股份有限公司、安策绩效大数据有限公司、爱石艺（广州）科技有限公司和艾欧史密斯（中国）热水器有限公司。

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，北京神州绿盟科技有限公司、北京启明星辰信息安全技术有限公司、新华三技术有限公司、北京天融信网络安全技术有限公司、安天科技集团股份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、联想集团、河南东方云盾信息技术有限公司、快页信息技术有限公司、安徽锋刃信息科技有限公司、中电智安科技有限公司、河南灵创电子科技有限公司、

河南信安世纪科技有限公司、亚信科技（成都）有限公司、中国电信股份有限公司上海研究院、信息产业信息安全测评中心、南京师范大学常州创新发展研究院软件与信息安全测评中心、软通动力信息技术（集团）股份有限公司、中孚安全技术有限公司、北京赛博昆仑科技有限公司、贵州泰若数字科技有限公司、国网安徽省电力有限公司、北京亿赛通科技发展有限责任公司、山石网科通信技术股份有限公司、杭州默安科技有限公司、云南联创网安科技有限公司、国网江西省电力有限公司电力科学研究院、江西和尔惠信息技术有限公司、广东盈世计算机科技有限公司、贵州华黔信安信息技术有限公司、西藏熙安信息技术有限责任公司、博智安全科技股份有限公司、北京君云天下科技有限公司、山东云天安全技术有限公司、郑州师范学院、超聚变数字技术有限公司、北京众安天下科技有限公司、北京山石网科信息技术有限公司、北京中关村实验室、南方电网数字电网集团信息通信科技有限公司、江苏云天网络安全技术有限公司、智网安云（武汉）信息技术有限公司、赛尔网络有限公司、交通运输信息安全中心有限公司、广东海事局、北京威努特技术有限公司、湖南省电子信息产业研究院及其他个人白帽子向 CNVD 提交了 13976 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、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 11596 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）	8211	8211
奇安信网神（补天平台）	2366	2366
北京神州绿盟科技有限公司	636	0
北京启明星辰信息安全技术有限公司	609	4
三六零数字安全科技集团有限公司	547	547
新华三技术有限公司	518	0
上海交大	472	472
北京天融信网络安全技术有限公司	290	5
安天科技集团股份有限公司	220	0
深信服科技股份有限公司	179	0

中国电信股份有限公司网络安全产品运营中心	143	143
阿里云计算有限公司	109	3
北京长亭科技有限公司	75	2
远江盛邦（北京）网络安全科技股份有限公司	45	45
北京数字观星科技有限公司	28	0
杭州迪普科技股份有限公司	24	0
中电科网络安全科技股份有限公司	7	7
京东科技信息技术有限公司	6	6
杭州安恒信息技术股份有限公司	6	6
北京信联数安科技有限公司	3	3
北京知道创宇信息技术有限公司	2	0
南京众智维信息科技有限公司	2	2
华为技术有限公司	2	2
西安四叶草信息技术有限公司	2	2
奇安星城网络安全运营服务（长沙）有限公司	127	127
联想集团	109	109
河南东方云盾信息技术有限公司	56	56
快页信息技术有限公	51	51

司		
安徽锋刃信息科技有限公司	30	30
中电智安科技有限公司	22	22
河南灵创电子科技有限公司	12	12
河南信安世纪科技有限公司	12	12
亚信科技（成都）有限公司	10	10
中国电信股份有限公司上海研究院	5	5
信息产业信息安全测评中心	4	4
南京师范大学常州创新发展研究院软件与信息安全测评中心	4	4
软通动力信息技术（集团）股份有限公司	4	4
中孚安全技术有限公司	3	3
北京赛博昆仑科技有限公司	3	3
贵州泰若数字科技有限公司	3	3
国网安徽省电力有限公司	2	2
北京亿赛通科技发展有限责任公司	2	2
山石网科通信技术股份有限公司	2	2
杭州默安科技有限公司	2	2

云南联创网安科技有限公司	2	2
国网江西省电力有限公司电力科学研究院	2	2
江西和尔惠信息技术有限公司	2	2
广东盈世计算机科技有限公司	2	2
贵州华黔信安信息技术有限公司	2	2
西藏熙安信息技术有限责任公司	2	2
博智安全科技股份有限公司	2	2
北京君云天下科技有限公司	1	1
山东云天安全技术有限公司	1	1
郑州师范学院	1	1
超聚变数字技术有限公司	1	1
北京众安天下科技有限公司	1	1
北京山石网科信息技术有限公司	1	1
北京中关村实验室	1	1
南方电网数字电网集团信息通信科技有限公司	1	1
江苏云天网络安全技术有限公司	1	1
智网安云（武汉）信息技术有限公司	1	1
赛尔网络有限公司	1	1
交通运输信息安全中	1	1

心有限公司		
广东海事局	1	1
北京威努特技术有限公司	1	1
湖南省电子信息产业研究院	1	1
CNCERT 宁夏分中心	5	5
CNCERT 河北分中心	5	5
CNCERT 贵州分中心	3	3
个人	1645	1645
报送总计	16652	13976

本周漏洞按类型和厂商统计

本周，CNVD 收录了 337 个漏洞。WEB 应用 127 个，应用程序 86 个，网络设备（交换机、路由器等网络端设备）66 个，数据库 20 个，安全产品 15 个，操作系统 14 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	127
应用程序	86
网络设备（交换机、路由器等网络端设备）	66
数据库	20
安全产品	15
操作系统	14
智能设备（物联网终端设备）	9

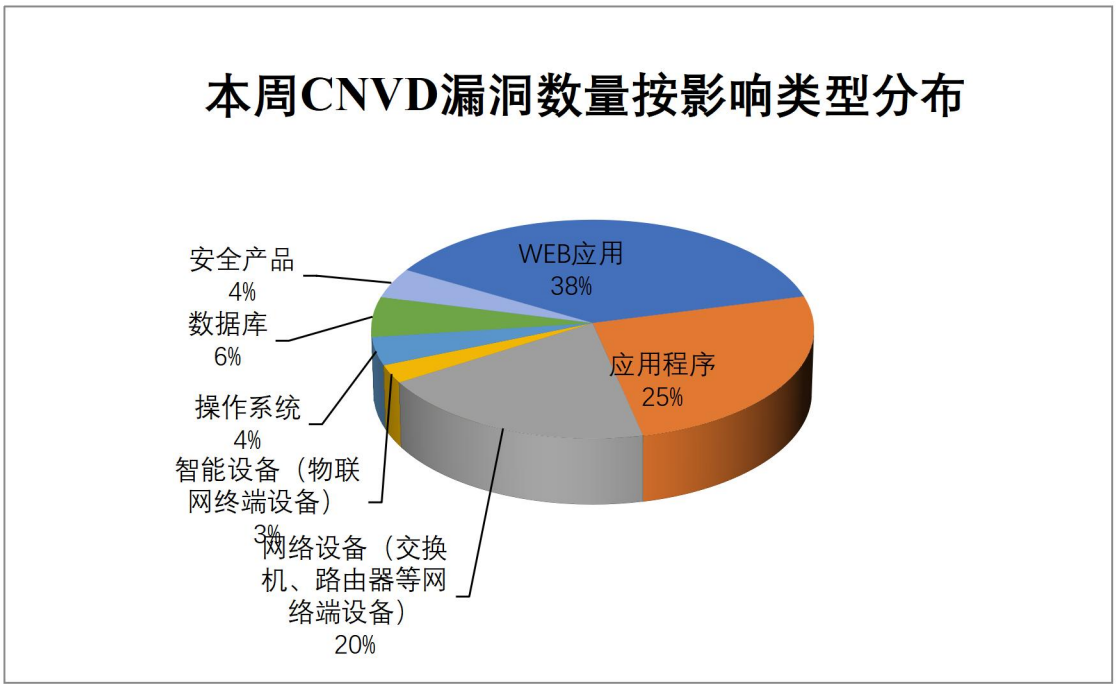

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 ScienceLogic、MileSight、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	ScienceLogic	24	7%
2	MileSight	20	6%
3	Oracle	20	6%
4	SAP	14	4%
5	Google	14	4%
6	Trend Micro	12	4%
7	DELL	11	3%
8	新华三技术有限公司	7	2%
9	D-Link	6	2%
10	其他	209	62%

本周行业漏洞收录情况

本周，CNVD 收录了 72 个电信行业漏洞，21 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，“D-Link DIR-895 身份验证绕过漏洞、Milesight UR32 L 缓冲区溢出漏洞”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/

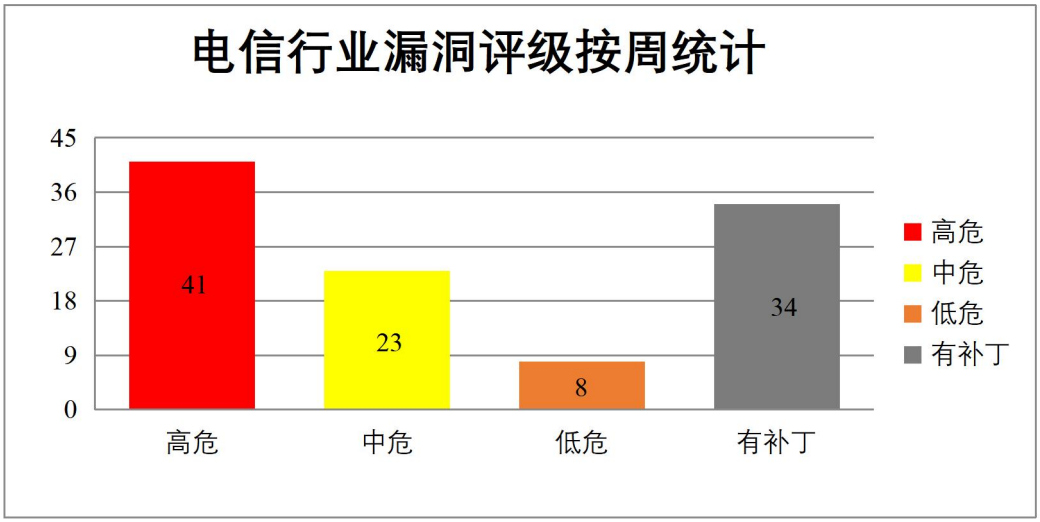

图 3 电信行业漏洞统计

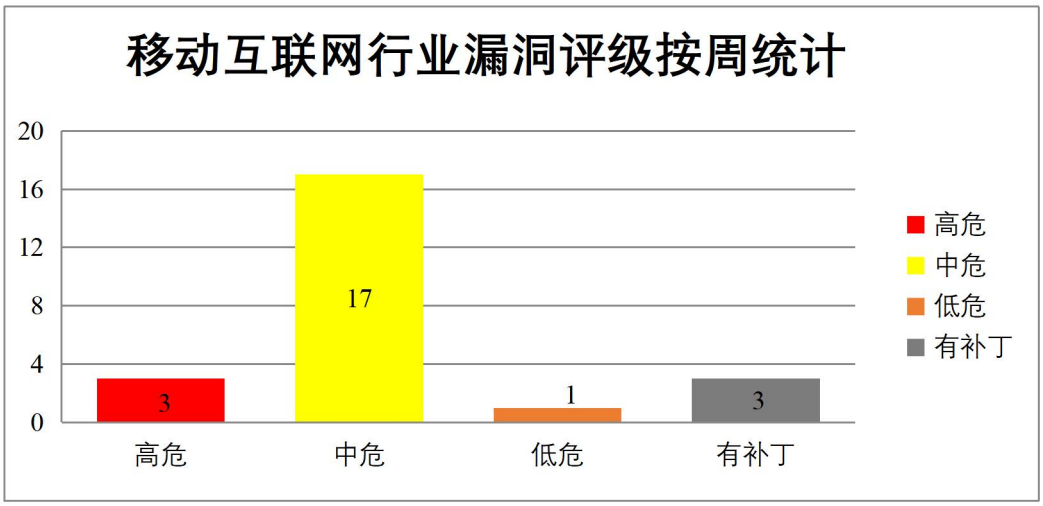

图 4 移动互联网行业漏洞统计

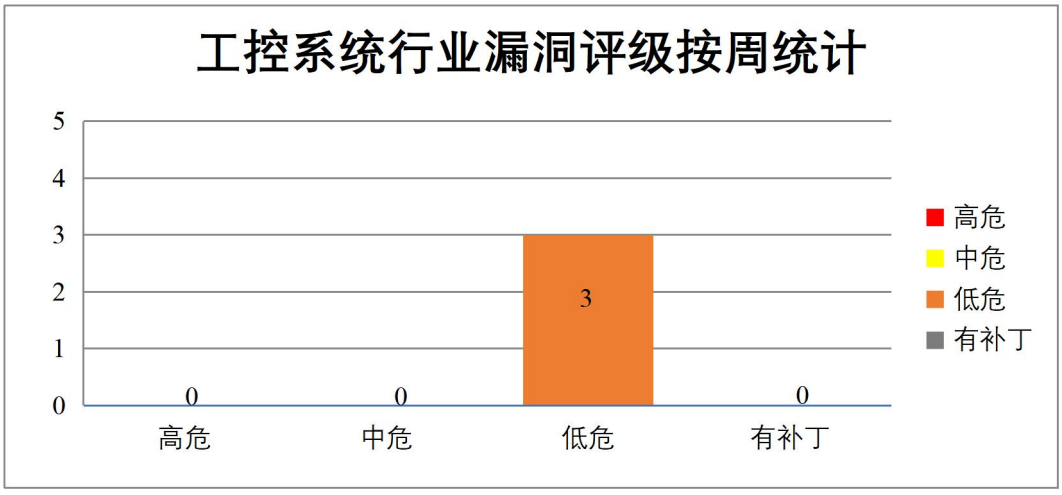

图 5 工控系统行业漏洞统计

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、DELL 产品安全漏洞

Dell PowerScale OneFS 是美国戴尔（Dell）公司的一个操作系统。提供横向扩展 NAS 的 PowerScale OneFS 操作系统。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞提升权限，导致拒绝服务，代码执行和信息泄露等。

CNVD 收录的相关漏洞包括：Dell PowerScale OneFS 保护机制绕过漏洞、Dell PowerScale OneFS 信息泄露漏洞（CNVD-2023-65214、CNVD-2023-65223）、Dell PowerScale OneFS 权限提升漏洞（CNVD-2023-65220、CNVD-2023-65218、CNVD-2023-65217、CNVD-2023-65221、CNVD-2023-65213）。其中，“Dell PowerScale OneFS 保护机制绕过漏洞”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-2023-65213
https://www.cnvd.org.cn/flaw/show/CNVD-2023-65216
https://www.cnvd.org.cn/flaw/show/CNVD-2023-65214
https://www.cnvd.org.cn/flaw/show/CNVD-2023-65220
https://www.cnvd.org.cn/flaw/show/CNVD-2023-65218
https://www.cnvd.org.cn/flaw/show/CNVD-2023-65217
https://www.cnvd.org.cn/flaw/show/CNVD-2023-65223
https://www.cnvd.org.cn/flaw/show/CNVD-2023-65221

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文件访问限制，执行任意代码，导致浏览器关闭等。

CNVD 收录的相关漏洞包括：Google Chrome 类型混淆漏洞（CNVD-2023-65154）、Google Chrome Skia 缓冲区溢出漏洞（CNVD-2023-65153）、Google Chrome Extensions 内存错误引用漏洞（CNVD-2023-65152）、Google Chrome 数据伪造问题漏洞（CNVD-2023-65156）、Google Chrome 输入验证错误漏洞（CNVD-2023-65155、CNVD-2023-65158）、Google Chrome 内存错误引用漏洞（CNVD-2023-65163、CNVD-2023-65162）。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-2023-65154
https://www.cnvd.org.cn/flaw/show/CNVD-2023-65153
https://www.cnvd.org.cn/flaw/show/CNVD-2023-65152
https://www.cnvd.org.cn/flaw/show/CNVD-2023-65156

https://www.cnvd.org.cn/flaw/show/CNVD-2023-65155

https://www.cnvd.org.cn/flaw/show/CNVD-2023-65158

https://www.cnvd.org.cn/flaw/show/CNVD-2023-65163

https://www.cnvd.org.cn/flaw/show/CNVD-2023-65162

3、SAP 产品安全漏洞

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 Host Agent 是一套支持操作系统监视、数据库监视和系统实例监视等多项生命周期管理任务的代理程序。SAP Supplier Relationship Management（SRM）是一套供应商关系管理解决方案。该产品实现了企业内以及供应商之间采购和购置流程的自动化，并提供发票开具等功能。SAP PowerDesigner 是一款数据库设计软件。SAP NetWeaver Process Integration（PI）是一套 SAP 企业应用程序集成软件，是 NetWeaver 产品组的一个组件。该组件主要用于内部系统与外部的信息交换。SAP NetWeaver Enterprise Portal 是一个 SAP NetWeaver 的 Web 前端组件。SAP Solution Manager 是一套集系统监控、SAP 支持桌面、自助服务、ASAP 实施等多个功能为一体的系统管理平台。该平台可以帮助客户建立 SAP 解决方案的生命周期管理，并提供系统监控、远程支持服务和 SAP 产品组件升级等功能。SAP NetWeaver 是德国思爱普（SAP）公司的一套面向服务的集成化应用平台。该平台主要为 SAP 应用程序提供开发和运行环境。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞注入恶意脚本或 HTML 代码，当恶意数据被查看时，可获取敏感信息或劫持用户会话，执行无目标 HTTP 请求，导致系统受损等。

CNVD 收录的相关漏洞包括：SAP Business One 信息泄露漏洞（CNVD-2023-65177）、SAP Host Agent 信息泄露漏洞（CNVD-2023-65176）、SAP Supplier Relationship Management 信息泄露漏洞、SAP PowerDesigner 访问控制错误漏洞、SAP NetWeaver Process Integration 访问控制错误漏洞（CNVD-2023-65180）、SAP NetWeaver Enterprise Portal 跨站脚本漏洞（CNVD-2023-65184）、SAP Solution Manager 代码问题漏洞、SAP NetWeaver 路径遍历漏洞（CNVD-2023-65181）。其中，“SAP PowerDesigner 访问控制错误漏洞、SAP NetWeaver 路径遍历漏洞（CNVD-2023-65181）”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-2023-65177

https://www.cnvd.org.cn/flaw/show/CNVD-2023-65176

https://www.cnvd.org.cn/flaw/show/CNVD-2023-65175

https://www.cnvd.org.cn/flaw/show/CNVD-2023-65174

https://www.cnvd.org.cn/flaw/show/CNVD-2023-65180

https://www.cnvd.org.cn/flaw/show/CNVD-2023-65184

https://www.cnvd.org.cn/flaw/show/CNVD-2023-65182

https://www.cnvd.org.cn/flaw/show/CNVD-2023-65181

4、Trend Micro 产品安全漏洞

Trend Micro Apex One 是美国趋势科技（Trend Micro）公司的一款终端防护软件。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞将任意文件上传到管理服务器，从而导致使用系统权限远程执行代码，提升权限，并将任意值写入代理子密钥等。

CNVD 收录的相关漏洞包括：Trend Micro Apex One 权限提升漏洞（CNVD-2023-65418、CNVD-2023-65417、CNVD-2023-65421、CNVD-2023-65420、CNVD-2023-65419、CNVD-2023-65424）、Trend Micro Apex One 访问控制错误漏洞（CNVD-2023-65422）、Trend Micro Apex One 路径遍历漏洞。其中，“Trend Micro Apex One 路径遍历漏洞”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-2023-65418

https://www.cnvd.org.cn/flaw/show/CNVD-2023-65417

https://www.cnvd.org.cn/flaw/show/CNVD-2023-65422

https://www.cnvd.org.cn/flaw/show/CNVD-2023-65421

https://www.cnvd.org.cn/flaw/show/CNVD-2023-65420

https://www.cnvd.org.cn/flaw/show/CNVD-2023-65419

https://www.cnvd.org.cn/flaw/show/CNVD-2023-65424

https://www.cnvd.org.cn/flaw/show/CNVD-2023-65423

5、TP-LINK Smart bulb Tapo series L530 和 Tapo Application 信息泄露漏洞

TP-LINK Smart bulb Tapo 是中国普联（TP-LINK）公司的一款智能灯泡。本周，TP-LINK Smart bulb Tapo series L530 和 Tapo Application 被披露存在信息泄露漏洞。攻击者可利用该漏洞通过 AES128-CBC 功能中的 IV 组件获取敏感信息。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-2023-66236

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-2023-65150	Google Chrome ANGLE 缓冲区溢出漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://chromereleases.googleblog.com/2023/08/stable-channel-update-for-desktop_15.html
CNVD-2023	Google Pixel 缓冲区溢出漏	高	厂商已发布了漏洞修复程序，请及

-65160	洞（CNVD-2023-65160）		时关注更新：https://source.android.com/docs/security/bulletin/pixel/2023-07-01?hl=zh-cn
CNVD-2023-65166	Adobe Dimension 堆缓冲区溢出漏洞（CNVD-2023-65166）	高	厂商已发布了漏洞修复程序，请及时关注更新:https://helpx.adobe.com/security/products/dimension/apsb23-44.html
CNVD-2023-65168	D-Link DIR-885L 身份验证绕过漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.dlink.com/en/security-bulletin/
CNVD-2023-65167	D-Link DIR-859 身份验证绕过漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.dlink.com/en/security-bulletin/
CNVD-2023-65179	SAP Message Server 授权问题漏洞	高	目前厂商已发布升级补丁以修复漏洞，详情请关注厂商主页：https://www.sap.com/documents/2022/02/fa865ea4-167e-0010-bca6-c68f7e60039b.html
CNVD-2023-65486	Milesight UR32L urvpn_client cmd_name_action 功能命令执行漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：https://www.milesight-iot.com/cellular/router/ur32l/
CNVD-2023-65498	Milesight UR32L libzebra.so bridge_group 功能命令注入漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：https://www.milesight-iot.com/cellular/router/ur32l/
CNVD-2023-65499	Milesight UR32L zebra vlan_name 功能命令注入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.milesight-iot.com/cellular/router/ur32l/
CNVD-2023-66411	ScienceLogic SL1 命令执行漏洞（CNVD-2023-66411）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://sciencelogic.com/platform/overview

小结：本周，DELL 产品被披露存在多个漏洞，攻击者可利用漏洞提升权限，导致拒绝服务，代码执行和信息泄露等。此外，Google、SAP、Trend Micro 等多款产品被披露存在多个漏洞，攻击者可利用漏洞注入恶意脚本或 HTML 代码，绕过文件访问限制，提升权限，执行任意代码等。另外，TP-LINK Smart bulb Tapo series L530 和 Tapo Application 被披露存在信息泄露漏洞。攻击者可利用漏洞通过 AES128-CBC 功能中的

IV 组件获取敏感信息。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、Bento4 拒绝服务漏洞（CNVD-2023-66174）

验证描述

Bento4 是一款用于读写 MP4 文件的开源的 C++库。

Bento4 存在拒绝服务漏洞，该漏洞源于 mp4crypt 中的 AP4_Processor::ProcessFragments 函数包含分段违规，攻击者可利用该漏洞导致拒绝服务攻击。

验证信息

POC 链接：https://github.com/axiomatic-systems/Bento4/issues/784

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2023-66174

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. Adobe ColdFusion 安全漏洞尽管有补丁，但仍被利用

Fortinet 观察到针对 Web 开发计算平台 Adobe ColdFusion 的威胁利用，此漏洞会导致任意代码执行。

参考链接：https://www.infosecurity-magazine.com/news/adobe-coldfusion-vulnerabilities/

2. Juniper 防火墙、Openfire 和 Apache RocketMQ 受到新漏洞的攻击

据多份报告称，最近披露的影响 Juniper 防火墙、Openfire 和 Apache RocketMQ 服务器的安全漏洞已被广泛利用。

参考链接：https://thehackernews.com/2023/08/alert-juniper-firewalls-openfire-and.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