国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2023 年 05 月 22 日-2023 年 05 月 28 日 **2023 年第 21 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 534 个，其中高危漏洞 228 个、中危漏洞 284 个、低危漏洞 22 个。漏洞平均分值为 6.36。本周收录的漏洞中，涉及 0day 漏洞 417 个（占 78%），其中互联网上出现“Hoosk CMS 任意文件上传漏洞、Resort Reservation System 跨站脚本漏洞”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 6973 个，与上周（15110 个）环比减少 54%。

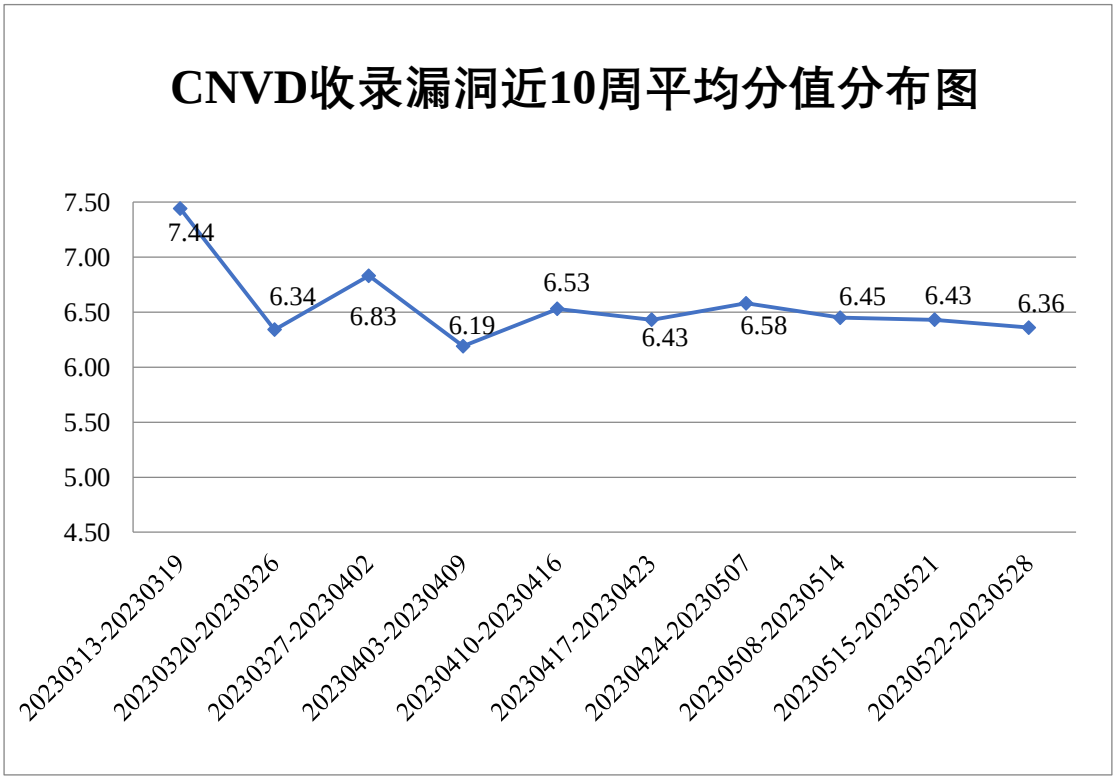

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 13 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 1168 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 234 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：

众瀛贸易集团有限公司、中农国华农业科技（北京）有限公司、中科宇图科技股份有限公司、中慈网络科技有限公司、郑州三晖电气股份有限公司、正奇晟业（北京）科技有限公司、正方软件股份有限公司、浙江中易慧能科技有限公司、长沙米拓信息技术有限公司、漳州市芗城帝兴软件开发有限公司、云易宿（北京）文旅科技有限公司、友讯电子设备（上海）有限公司、用友网络科技股份有限公司、易丞（北京）信息服务有限公司、迅全信息科技（上海）有限公司、西安瑞友信息技术资讯有限公司、武汉长光科技有限公司、武汉云贝网络科技有限公司、武汉烽火信息集成技术有限公司、网宿科技股份有限公司、网经科技（苏州）有限公司、天津市神州商龙科技股份有限公司、天津出行有限公司、苏州汇川技术有限公司、四川奇石缘科技股份有限公司、施耐德电气（中国）有限公司、深圳中赫斯曼科技有限公司、深圳友联科技有限公司、深圳市万网博通科技有限公司、深圳市万普拉斯科技有限公司、深圳市捷诚速通供应链有限公司、深圳市吉祥腾达科技有限公司、深圳市必联电子有限公司、上海卓卓网络科技有限公司、上海复翼软件开发有限公司、上海泛微网络科技股份有限公司、上海百胜软件股份有限公司、上海阿法迪智能数字科技股份有限公司、陕西凯星电子科技有限责任公司、山东中维世纪科技股份有限公司、山东龙帝科技发展有限公司、山东国通智云实业集团有限公司、厦门市灵鹿谷科技有限公司、泉州市云语信息技术有限公司、青岛积成电子股份有限公司、青岛东软载波科技股份有限公司、普元信息技术股份有限公司、普联技术有限公司、南宁迈世信息技术有限公司、南京致汇达网络科技有限公司、弥特盈泰（广州）软件科技有限公司、梦想 CMS、蚂蚁科技集团股份有限公司、洛阳宏兴石化销售有限公司、联合见智科技有限公司、力合科技（湖南）股份有限公司、兰州泰力电子科技有限公司、科来网络技术股份有限公司、敬业钢铁有限公司、吉翁电子（深圳）有限公司、惠普贸易（上海）有限公司、和利时信安院、合肥天寻信息科技有限公司、合肥泛米智能科技有限公司、合肥贰道网络科技有限公司、杭州雄伟科技开发股份有限公司、杭州三汇信息工程有限公司、杭州科强信息技术有限公司、杭州飞致云信息科技有限公司、杭州迪普科技股份有限公司、汉王科技股份有限公司、广州中望龙腾软件股份有限公司、广州云养邦互联科技有限公司、广州市国万电子科技有限公司、广州市保伦电子有限公司、广州南方卫星导航仪器有限公司、广联达科技股份有限公司、广东鼎易建筑科技有

限公司、广东保伦电子股份有限公司、福州网钛软件科技有限公司、方心科技股份有限公司、东北师大理想软件股份有限公司、顶点软件股份有限公司、帝国软件、创维集团有限公司、成都索贝数码科技股份有限公司、畅捷通信息技术股份有限公司、博世（中国）投资有限公司、北京中位科技有限公司、北京中成科信科技发展有限公司、北京因酷时代科技有限公司、北京亿思摩博网络科技有限公司、北京世纪超星信息技术发展有限责任公司、北京神州数码云科信息技术有限公司、北京神州视翰科技有限公司、北京前沿信安科技股份有限公司、北京米尔伟业科技有限公司、北京梦见星科技有限公司、北京宏达一甲教育科技有限公司、北京好雨科技有限公司、北京翰博尔信息技术股份有限公司、北京百卓网络技术有限公司、北京安兔兔科技有限公司、保汇通（厦门）网络科技有限公司、安元科技股份有限公司、安徽德拓信息科技有限公司、阿里巴巴集团安全应急响应中心和 BEESCMS。

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、阿里云计算有限公司、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。快页信息技术有限公司、北京升鑫网络科技有限公司、上海齐同信息科技有限公司、重庆电信系统集成公司、河南东方云盾信息技术有限公司、河南信安世纪科技有限公司、联想集团、安徽锋刃信息科技有限公司、内蒙古洞明科技有限公司、贵州泰若数字科技有限公司、浙江木链物联网科技有限公司、杭州默安科技有限公司、杭州美创科技有限公司、赛尔网络有限公司、江苏天竞云合数据技术有限公司、北京时代新威信息技术有限公司、海南神州希望网络有限公司、中国电信股份有限公司上海研究院、北京山石网科信息技术有限公司、北京六方云信息技术有限公司、合肥梆梆信息科技有限公司、中科国宏科技有限公司、北京君云天下科技有限公司、天津市兴先道科技有限公司、河北锘远网络科技有限公司、河南财政金融学院、国网智能电网研究院有限公司、任子行网络技术股份有限公司、黑龙江亿林网络股份有限公司、辽宁省烟草公司营口市公司、北京微步在线科技有限公司、德国电信咨询公司中国区公司、深圳市智安网络有限公司、重庆易阅科技有限公司、超聚变数字技术有限公司、河南灵创电子科技有限公司、交通运输信息安全中心有限公司（TISEC 洪椒战队）、福建中信网安信息科技有限公司、山东正中信息技术股份有限公司、神州灵云（北京）科技有限公司、宁夏凯信特信息科技有限公司、广州安亿信软件科技有限公司、北京安帝科技有限公司、郑州埃文科技、泸州职业技术学院、信联科技（南京）有限公司、北京水木羽林科技有限公司、软极网络技术（北京）有限公司及其他个人白帽子向 CNVD 提交了 6973 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）、斗象科技（漏洞盒子）、三六零数字安全科技集团有限公司和上海交大向 CNVD 共享的白帽子报送

的 4213 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）	1818	1818
斗象科技（漏洞盒子）	1483	1483
三六零数字安全科技集团有限公司	715	715
新华三技术有限公司	330	0
深信服科技股份有限公司	323	1
安天科技集团股份有限公司	306	1
上海交大	197	197
阿里云计算有限公司	183	1
北京神州绿盟科技有限公司	137	2
北京启明星辰信息安全技术有限公司	104	14
北京数字观星科技有限公司	89	0
天津市国瑞数码安全系统股份有限公司	59	0
杭州安恒信息技术股份有限公司	44	44
南京众智维信息科技有限公司	40	40
北京长亭科技有限公司	30	3
京东科技信息技术有限公司	24	7
杭州迪普科技股份有限公司	14	0
北京智游网安科技有限公司	7	7

北京天融信网络安全技术有限公司	4	4
浙江大华技术股份有限公司	4	4
北京知道创宇信息技术股份有限公司	2	0
卫士通信息产业股份有限公司	1	1
北京信联数安科技有限公司	1	1
中国电信股份有限公司网络安全产品运营中心	1	1
中国电信集团系统集成有限责任公司	1	1
远江盛邦（北京）网络安全科技股份有限公司	1	1
快页信息技术有限公司	205	205
北京升鑫网络科技有限公司	51	51
上海齐同信息科技有限公司	45	45
重庆电信系统集成公司	44	44
河南东方云盾信息技术有限公司	40	40
河南信安世纪科技有限公司	36	36
联想集团	28	28
安徽锋刃信息科技有限公司	15	15
内蒙古洞明科技有限公司	14	14

贵州泰若数字科技有限公司	8	8
浙江木链物联网科技有限公司	7	7
杭州默安科技有限公司	7	7
杭州美创科技有限公司	7	7
赛尔网络有限公司	5	5
江苏天竞云合数据技术有限公司	5	5
北京时代新威信息技术有限公司	4	4
海南神州希望网络有限公司	4	4
中国电信股份有限公司上海研究院	3	3
北京山石网科信息技术有限公司	2	2
北京六方云信息技术有限公司	2	2
合肥梆梆信息科技有限公司	2	2
中科国宏科技有限公司	2	2
北京君云天下科技有限公司	2	2
天津市兴先道科技有限公司	2	2
河北镌远网络科技有限公司	2	2
河南财政金融学院	2	2
国网智能电网研究院有限公司	2	2
任子行网络技术股份	1	1

有限公司		
黑龙江亿林网络股份有限公司	1	1
辽宁省烟草公司营口市公司	1	1
北京微步在线科技有限公司	1	1
德国电信咨询公司中国区公司	1	1
深圳市智安网络有限公司	1	1
重庆易阅科技有限公司	1	1
超聚变数字技术有限公司	1	1
河南灵创电子科技有限公司	1	1
交通运输信息安全中心有限公司（TISEC洪椒战队）	1	1
福建中信网安信息科技有限公司	1	1
山东正中信息技术股份有限公司	1	1
神州灵云（北京）科技有限公司	1	1
宁夏凯信特信息科技有限公司	1	1
广州安亿信软件科技有限公司	1	1
北京安帝科技有限公司	1	1
郑州埃文科技	1	1
泸州职业技术学院	1	1
信联科技（南京）有	1	1

限公司		
北京水木羽林科技有限公司	1	1
软极网络技术（北京）有限公司	1	1
CNCERT 广西分中心	13	13
CNCERT 贵州分中心	4	4
个人	2043	2043
报送总计	8545	6973

本周漏洞按类型和厂商统计

本周，CNVD 收录了 534 个漏洞。WEB 应用 287 个，应用程序 138 个，网络设备（交换机、路由器等网络端设备）72 个，区块链 17 个，智能设备（物联网终端设备）7 个，安全产品 5 个，操作系统 4 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	287
应用程序	138
网络设备（交换机、路由器等网络端设备）	72
区块链	17
智能设备（物联网终端设备）	7
安全产品	5
操作系统	4
数据库	4

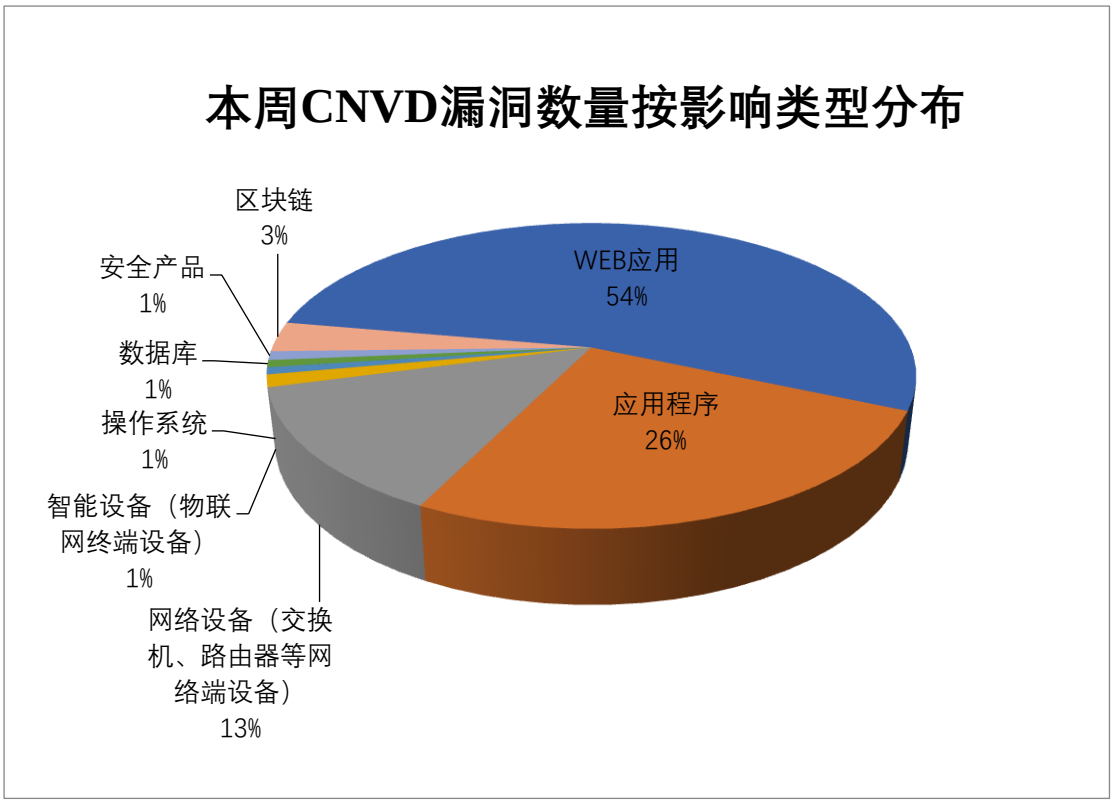

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Adobe、北京金和网络股份有限公司、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	Adobe	41	8%
2	北京金和网络股份有限公司	17	3%
3	SAP	15	3%
4	深圳维盟科技股份有限公司	15	3%
5	Cisco	14	3%
6	TOTOLINK	12	2%
9	H3C	12	2%
7	Schneider Electric	9	2%
8	广州红帆科技有限公司	8	1%
10	其他	391	73%

本周行业漏洞收录情况

本周，CNVD 收录了 58 个电信行业漏洞，46 个移动互联网行业漏洞，8 个工控行

业漏洞（如下图所示）。其中，“TOTOLINK X5000R 存在命令执行漏洞（CNVD-2023-40539）、Cisco Small Business 拒绝服务漏洞（CNVD-2023-40906）、Schneider Electric SoMachine HVAC 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/

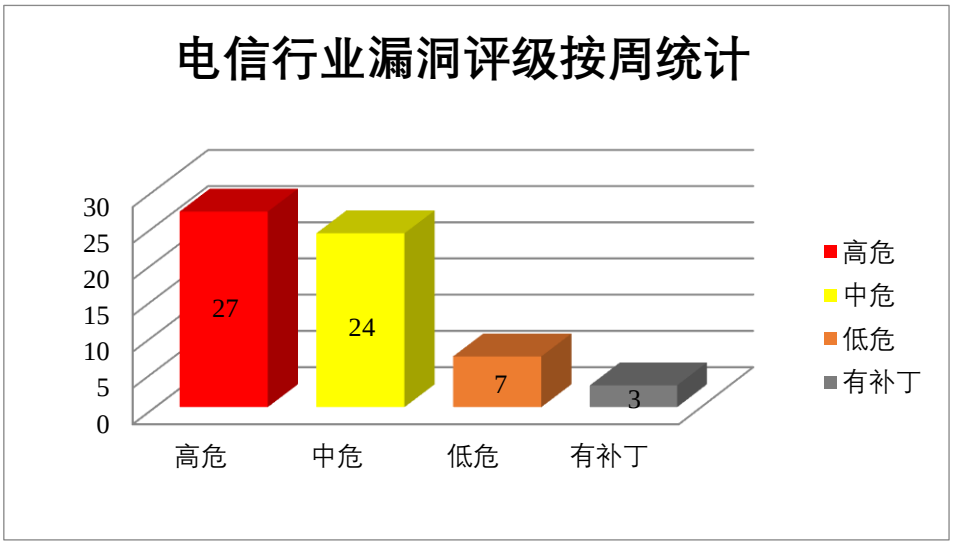

图 3 电信行业漏洞统计

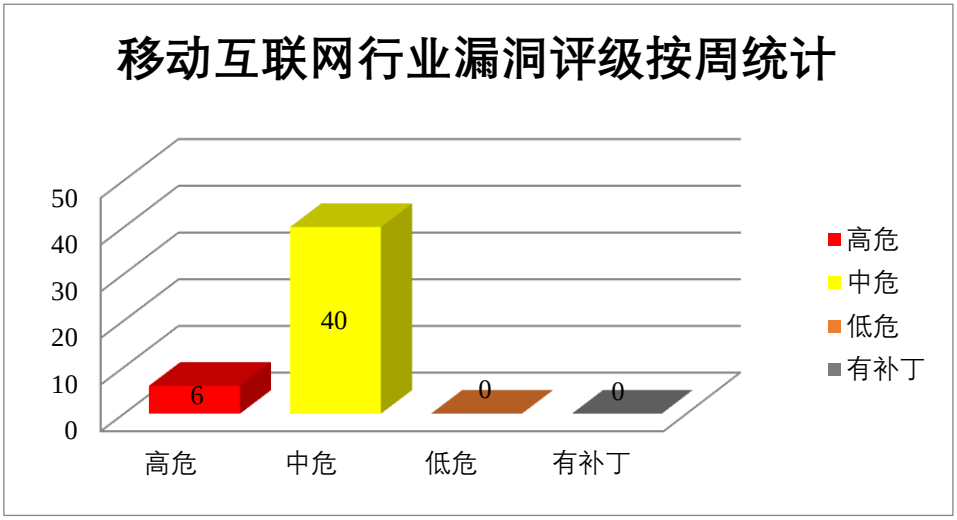

图 4 移动互联网行业漏洞统计

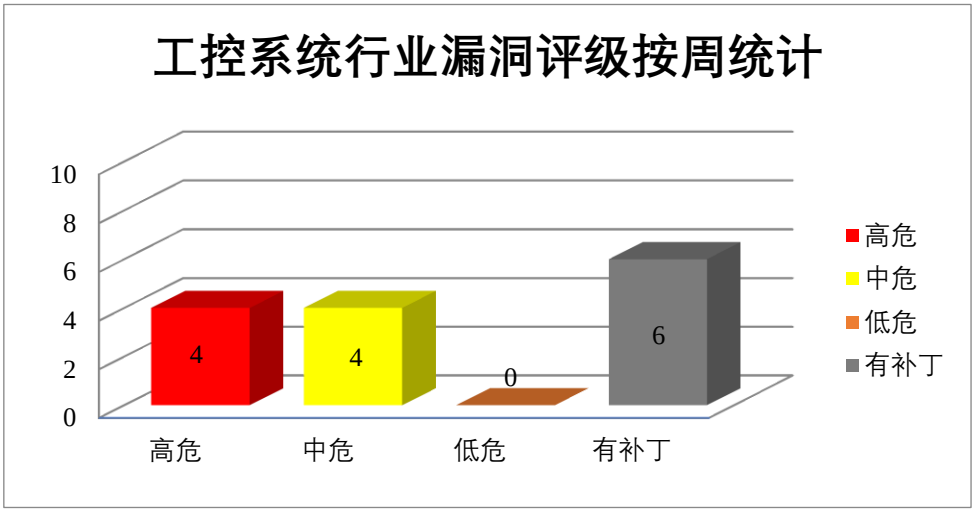

图 5 工控系统行业漏洞统计

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、 Adobe 产品安全漏洞

Adobe Substance 3D Painter 是美国奥多比（Adobe）公司的一个 3D 纹理处理应用程序。Adobe Dimension 是美国奥多比（Adobe）公司的一套 2D 和 3D 合成设计工具。本周，上述产品被披露存在越界读取漏洞，攻击者可利用漏洞执行任意代码。

CNVD 收录的相关漏洞包括：Adobe Substance 3D Painter 越界读取漏洞（CNVD-2023-40147、CNVD-2023-40146、CNVD-2023-40149、CNVD-2023-40152、CNVD-2023-41408）、Adobe Dimension 越界读取漏洞（CNVD-2023-41413、CNVD-2023-41416、CNVD-2023-41414）。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-2023-40147

https://www.cnvd.org.cn/flaw/show/CNVD-2023-40146

https://www.cnvd.org.cn/flaw/show/CNVD-2023-40149

https://www.cnvd.org.cn/flaw/show/CNVD-2023-40152

https://www.cnvd.org.cn/flaw/show/CNVD-2023-41408

https://www.cnvd.org.cn/flaw/show/CNVD-2023-41413

https://www.cnvd.org.cn/flaw/show/CNVD-2023-41416

https://www.cnvd.org.cn/flaw/show/CNVD-2023-41414

2、 Cisco 产品安全漏洞

Cisco Identity Services Engine（ISE）是美国思科（Cisco）公司的一款环境感知平台（ISE 身份服务引擎）。该平台通过收集网络、用户和设备中的实时信息，制定并实

施相应策略来监管网络。Cisco Small Business 是美国思科（Cisco）公司的一个交换机。Cisco DNA Center 是美国思科（Cisco）公司的一个网络管理和命令中心服务。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞从受影响设备的文件系统下载任意文件，对底层操作系统执行命令注入攻击，并将权限提升到 root 等。

CNVD 收录的相关漏洞包括：Cisco Identity Services Engine 命令注入漏洞（CNVD-2023-40185、CNVD-2023-40187）、Cisco Identity Services Engine 路径遍历漏洞（CNVD-2023-40184、CNVD-2023-40186）、Cisco Identity Services Engine 授权绕过漏洞（CNVD-2023-40191）、Cisco Identity Services Engine 任意文件下载漏洞、Cisco Small Business 拒绝服务漏洞（CNVD-2023-40906）、Cisco DNA Center 命令执行漏洞。其中，“Cisco Identity Services Engine 命令注入漏洞（CNVD-2023-40187）、Cisco Small Business 拒绝服务漏洞（CNVD-2023-40906）”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-2023-40185
https://www.cnvd.org.cn/flaw/show/CNVD-2023-40184
https://www.cnvd.org.cn/flaw/show/CNVD-2023-40187
https://www.cnvd.org.cn/flaw/show/CNVD-2023-40186
https://www.cnvd.org.cn/flaw/show/CNVD-2023-40191
https://www.cnvd.org.cn/flaw/show/CNVD-2023-40190
https://www.cnvd.org.cn/flaw/show/CNVD-2023-40906
https://www.cnvd.org.cn/flaw/show/CNVD-2023-41500

3、SAP 产品安全漏洞

SAP Application Interface Framework（SAP AIF）是德国思爱普（SAP）公司的一个应用程序接口框架。SAP BusinessObjects Platform 是德国思爱普（SAP）公司的一个用于数据报告、可视化和共享的集中式套件。SAP Web Dispatcher 是德国思爱普（SAP）公司的 Load Balancing 的核心组件，支持负载均衡，提供反向代理的功能，使得外网用户可以访问到内部应用。SAP NetWeaver AS 是德国思爱普（SAP）公司的一款 SAP 网络应用服务器。它不仅能提供网络服务，且还是 SAP 软件的基本平台。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，覆盖操作系统文件，导致系统不可用等。

CNVD 收录的相关漏洞包括：SAP Application Interface Framework 信息泄露漏洞、SAP BusinessObjects Platform 信息泄露漏洞、SAP Web Dispatcher 访问控制错误漏洞、SAP NetWeaver AS 资源管理错误漏洞、SAP NetWeaver AS 访问控制错误漏洞（CNVD-2023-40162）、SAP NetWeaver AS 跨站脚本漏洞（CNVD-2023-40169）、SAP NetWeaver AS 路径遍历漏洞、SAP BusinessObjects Business Intelligence Platform 信息泄

露漏洞（CNVD-2023-40166）。其中，“SAP NetWeaver AS 路径遍历漏洞、SAP BusinessObjects Business Intelligence Platform 信息泄露漏洞（CNVD-2023-40166）”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-2023-40161
https://www.cnvd.org.cn/flaw/show/CNVD-2023-40160
https://www.cnvd.org.cn/flaw/show/CNVD-2023-40164
https://www.cnvd.org.cn/flaw/show/CNVD-2023-40163
https://www.cnvd.org.cn/flaw/show/CNVD-2023-40162
https://www.cnvd.org.cn/flaw/show/CNVD-2023-40169
https://www.cnvd.org.cn/flaw/show/CNVD-2023-40168
https://www.cnvd.org.cn/flaw/show/CNVD-2023-40166

4、Schneider Electric 产品安全漏洞

Schneider Electric Conext Gateway 是法国施耐德电气（Schneider Electric）公司的一系列网关设备。Schneider Electric EcoStruxure Control Expert 是法国施耐德电气（Schneider Electric）公司的一套用于 Schneider Electric 逻辑控制器产品的编程软件。Schneider Electric Easy UPS Online Monitoring Software 是法国施耐德电气（Schneider Electric）公司的一款电源监控软件。Schneider Electric Easergy Builder 是法国施耐德电气（Schneider Electric）公司的一套用于 Easergy 远程终端单元和控制器的配置软件。Schneider Electric SoMachine HVAC 是法国施耐德电气（Schneider Electric）公司的一套专用于 Schneider Electric 逻辑控制器的编程软件。Schneider Electric Conext ComBox 是法国施耐德电气（Schneider Electric）公司的一款通信和监控设备。Schneider Electric OPC Factory Server 是法国施耐德电气（Schneider Electric）公司的一种软件应用程序。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞对文件系统进行未经授权的读取访问，执行任意代码，导致拒绝服务等。

CNVD 收录的相关漏洞包括：Schneider Electric Conext Gateway 输入验证错误漏洞、Schneider Electric EcoStruxure Control Expert 拒绝服务漏洞、Schneider Electric EcoStruxure Control Expert 代码执行漏洞、Schneider Electric Easy UPS Online Monitoring Software 访问控制错误漏洞、Schneider Electric Easergy Builder 代码问题漏洞、Schneider Electric SoMachine HVAC 缓冲区溢出漏洞、Schneider Electric Conext ComBox 跨站请求伪造漏洞、Schneider Electric OPC Factory Server XML 外部实体注入漏洞。其中，除“Schneider Electric EcoStruxure Control Expert 拒绝服务漏洞、Schneider Electric Easergy Builder 代码问题漏洞、Schneider Electric OPC Factory Server XML 外部实体注入漏洞”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-2023-40173
https://www.cnvd.org.cn/flaw/show/CNVD-2023-40177
https://www.cnvd.org.cn/flaw/show/CNVD-2023-40176
https://www.cnvd.org.cn/flaw/show/CNVD-2023-40175
https://www.cnvd.org.cn/flaw/show/CNVD-2023-40174
https://www.cnvd.org.cn/flaw/show/CNVD-2023-40179
https://www.cnvd.org.cn/flaw/show/CNVD-2023-40178
https://www.cnvd.org.cn/flaw/show/CNVD-2023-41536

5、TOTOLINK A3300R 命令注入漏洞

TOTOLINK A3300R 是中国吉翁电子（TOTOLINK）公司的一款无线路由器。本周，TOTOLINK A3300R 被披露存在命令注入漏洞。该漏洞源于请求/cgi-bin/cstecgi.cgi 的 setddnscfg 函数未能正确过滤构造命令特殊字符、命令等。攻击者可利用该漏洞导致任意命令执行。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-2023-41866

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-2023-40574	Linux kernel 拒绝服务漏洞（CNVD-2023-40574）	高	厂商已发布了漏洞修复程序，请及时关注更新: https://bugzilla.redhat.com/show_bug.cgi?id=2196292
CNVD-2023-40603	IBM Spectrum Virtualize 信息泄露漏洞（CNVD-2023-40603）	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/6985697
CNVD-2023-40915	OpenEMR 访问控制错误漏洞（CNVD-2023-40915）	高	厂商已发布了漏洞修复程序，请及时关注更新： https://github.com/openemr/openemr/commit/953cb84dfd55fee9d5296668ec7fdb8bf25bcea4
CNVD-2023-41401	GitLab CE/EE 路径遍历漏洞	高	用户可参考如下供应商提供的安全公告获得补丁信息： https://about.gitlab.com/releases/2023/05/23/critical-security-release-gitlab-16-0-1-released/
CNVD-2023	Adobe Dimension 堆栈缓冲	高	厂商已发布了漏洞修复程序，请及

-41419	区溢出漏洞		时关注更新：https://helpx.adobe.com/security/products/dimension/apsb23-20.html
CNVD-2023-41497	Prestashop 路径遍历漏洞（CNVD-2023-41497）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/PrestaShop/PrestaShop/releases/tag/8.0.4
CNVD-2023-41537	Rockwell Automation ThinManager 加密问题漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1139442
CNVD-2023-41863	PHPOK 代码问题漏洞	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.phpok.com/phpok.html
CNVD-2023-41861	SQLite 代码注入漏洞	高	目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载：https://github.com/xerial/sqlite-jdbc/security/advisories/GHSA-6phf-6h5g-97j2
CNVD-2023-41864	SEMCMS SQL 注入漏洞（CNVD-2023-41864）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.sem-cms.cn/wenda/view-56.html

小结：本周，Adobe 产品被披露存在多个漏洞，攻击者可利用漏洞执行任意代码。此外，Cisco、SAP、Schneider Electric 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，覆盖操作系统文件，执行任意代码，导致拒绝服务等。另外，TOTOLINK A3300R 被披露存在命令注入漏洞。攻击者可利用该漏洞导致任意命令执行。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、Hoosk CMS 任意文件上传漏洞

验证描述

Hoosk CMS 是一个轻量级的内容管理系统。

Hoosk CMS v1.8.0 版本存在任意文件上传漏洞，该漏洞源于其/attachments 组件对上传的文件未能进行有效的验证。攻击者可利用漏洞远程执行代码。

验证信息

POC 链接：https://github.com/havok89/Hoosk/issues/64

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2023-40181

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. D-Link 修复了 D-View 8 网络管理套件中的两个安全漏洞

D-Link 修复了其 D-View 8 网络管理套件中的两个安全漏洞，这两个漏洞可能导致未经身份验证的攻击者绕过和执行任意代码。

参考链接：https://securityaffairs.com/146667/security/d-link-critical-flaws-d-view-8.html

2. Zyxel 防火墙和 VPN 设备受到安全漏洞的影响

Zyxel 修复了多个防火墙和 VPN 产品中的两个安全漏洞，这两个漏洞可能导致远程代码执行或导致 DoS 情况。

参考链接：https://securityaffairs.com/146660/security/zyxel-firewall-vpn-critical-flaw.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