国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2023 年 03 月 27 日-2023 年 04 月 02 日　　2023 年第 13 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 246 个，其中高危漏洞 141 个、中危漏洞 90 个、低危漏洞 15 个。漏洞平均分值为 6.83。本周收录的漏洞中，涉及 0day 漏洞 198 个（占 80%），其中互联网上出现“Simmeth System Supplier Manager SQL 注入漏洞、Eolinker 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 24061 个，与上周（16489 个）环比增加 46%。

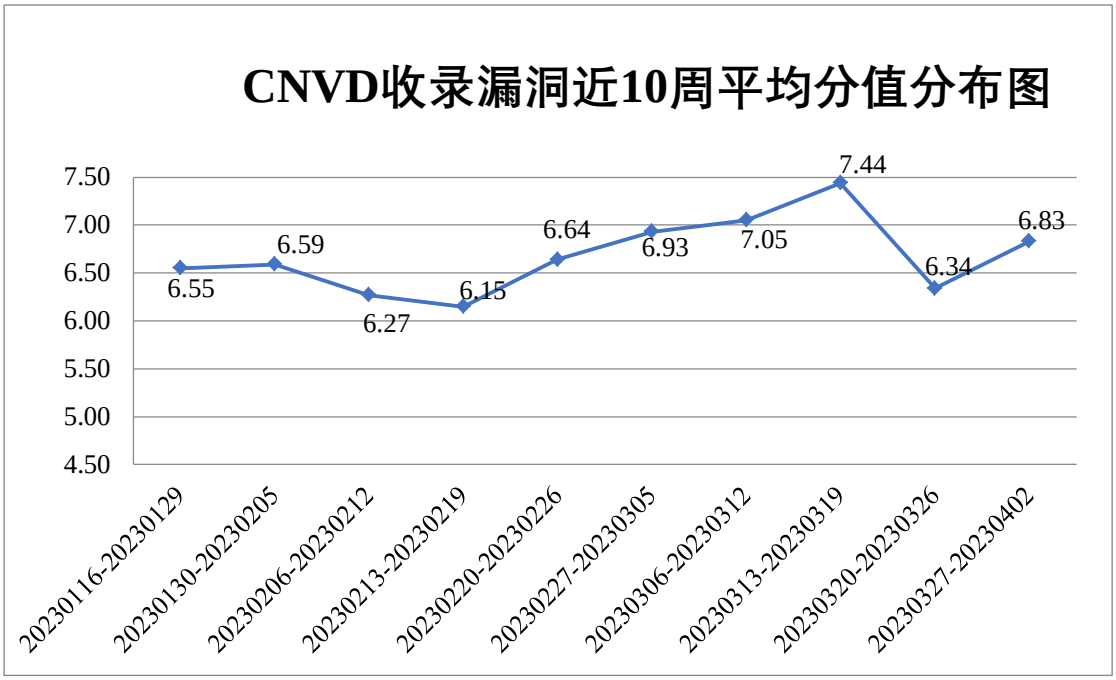

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 29 起，向基础电

信企业通报漏洞事件 108 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 1098 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 204 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 117 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、中民智金科技股份有限公司、浙江宇视科技有限公司、漳州市芗城帝兴软件开发有限公司、友讯电子设备（上海）有限公司、用友网络科技股份有限公司、阳光智园科技有限公司、天津天堰科技股份有限公司、天津神州浩天科技有限公司、天地伟业技术有限公司、神彩科技股份有限公司、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、深圳市同为数码科技股份有限公司、深圳市思迅软件股份有限公司、深圳市锐明技术股份有限公司、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、深圳市卡方通用科技开发有限公司、深圳市捷道智控实业有限公司、深圳市合信自动化技术有限公司、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、上海展盟网络科技有限公司、上海商创网络科技有限公司、上海聚均科技有限公司、上海寰创通信科技股份有限公司、上海保利物业酒店管理集团有限公司、上海阿法迪智能数字科技股份有限公司、熵基科技股份有限公司、商派软件有限公司、山脉科技股份有限公司、山东中创软件商用中间件股份有限公司、山东运筹软件有限公司、山东云时空信息科技有限公司、山东威尔数据股份有限公司、山东科德电子有限公司、厦门网中网软件有限公司、厦门四信通信科技有限公司、厦门海为科技有限公司、任子行网络技术股份有限公司、全讯汇聚网络科技（北京）有限公司、普联技术有限公司、鹏为软件股份有限公司、南京涌亿思信息技术有限公司、南京擎盾信息科技有限公司、南京爱普雷德电子科技有限公司、南昌腾速科技有限公司、梅州市青云客网络科技有限公司、迈普通信技术股份有限公司、乐鑫信息科技（上海）股份有限公司、朗坤智慧科技股份有限公司、科来网络技术股份有限公司、江西金磊科技发展有限公司、江苏优度软件有限公司、江苏汇文软件有限公司、江苏国光信息产业股份有限公司、济南大森制冷设备有限公司、吉翁电子（深圳）有限公司、怀化南山田舍科技有限公司、湖北易都信息技术有限公司、鸿生汇引（北京）文化传播有限公司、杭州智果科技有限公司、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、杭州玳数科技有限公司、汉王科技股份有限公司、广州市花都区新华伟创广告设计服务部、广州好象科技有限公司、甘肃成兴信息科技有限公司、飞天站群系统、呆错建站系统、畅捷通信息技术股份有限公司、北京中创视讯科技有限公司、北京云帆互联网科技有限公司、北京亚鸿世纪科技发展有限公司、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、北京现代汽车有限公司、北京万户网络技术有限公司、北京通达信科科技有限公司、北京如易行科技有限公司、北京普诺迪信息系统技术研发有限

责任公司、北京欧倍尔软件技术开发有限公司、北京梦见星科技有限公司、北京朗新天霁软件技术有限公司、北京竞业达数码科技股份有限公司、北京鲸榄网络科技有限公司、北京金盘鹏图软件技术有限公司、北京和利时集团、北京国炬信息技术有限公司、北京东尚泰和科技有限公司、北京大为知创科技有限公司、北京北信源软件股份有限公司、北京百卓网络技术有限公司、安徽中技国医医疗有限公司、安徽中技国医医疗科技有限公司和安徽旭帆信息科技有限公司。

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、北京启明星辰信息安全技术有限公司、阿里云计算有限公司、安天科技集团股份有限公司、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、贵州泰若数字科技有限公司、北京山石网科信息技术有限公司、博智安全科技股份有限公司、北京升鑫网络科技有限公司、湖南轻山信息技术有限公司、山东鼎夏智能科技有限公司、安徽锋刃信息科技有限公司、杭州美创科技有限公司、浙江安腾信息技术有限公司、河南东方云盾信息技术有限公司、中孚安全技术有限公司、杭州默安科技有限公司、河南信安世纪科技有限公司、北京远禾科技有限公司、山东九域信息技术有限公司、任子行网络技术股份有限公司、上海齐同信息科技有限公司、广州安亿信软件科技有限公司、汇安云（山东）信息科技有限公司、北京云科安信科技有限公司（Seraph 安全实验室）、苏州棱镜七彩信息科技有限公司、山东新潮信息技术有限公司、赛尔网络有限公司、北京威努特技术有限公司、上海市信息安全测评认证中心、中科国宏科技有限公司、上海天存信息技术有限公司、云南联创网安科技有限公司、内蒙古中叶信息技术有限责任公司、北京珞安科技有限责任公司、京数安（北京）科技有限公司、郑州埃文科技、河南灵创电子科技有限公司、信息产业信息安全测评中心及其他个人白帽子向 CNVD 提交了 24061 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）、奇安信网神（补天平台）、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 20146 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）	15914	15914
奇安信网神（补天平台）	3079	3079
新华三技术有限公司	791	0
上海交大	732	732
三六零数字安全科技	421	421

集团有限公司		
北京启明星辰信息安全技术有限公司	368	0
阿里云计算有限公司	281	18
安天科技集团股份有限公司	278	0
北京神州绿盟科技有限公司	259	0
杭州安恒信息技术股份有限公司	181	181
远江盛邦（北京）网络安全科技股份有限公司	166	166
天津市国瑞数码安全系统股份有限公司	118	0
北京数字观星科技有限公司	99	0
中国电信集团系统集成有限责任公司	32	6
京东科技信息技术有限公司	23	2
杭州迪普科技股份有限公司	14	0
深信服科技股份有限公司	4	4
北京知道创宇信息技术股份有限公司	3	0
西安四叶草信息技术有限公司	1	1
北京信联数安科技有限公司	1	1
北京天融信网络安全技术有限公司	1	1
北京华顺信安信息技术有限公司	308	0

快页信息技术有限公司	302	302
贵州泰若数字科技有限公司	262	262
北京山石网科信息技术有限公司	173	173
博智安全科技股份有限公司	116	116
北京升鑫网络科技有限公司	67	67
湖南轻山信息技术有限公司	64	64
山东鼎夏智能科技有限公司	41	41
安徽锋刃信息科技有限公司	25	25
杭州美创科技有限公司	24	24
浙江安腾信息技术有限公司	22	22
河南东方云盾信息技术有限公司	20	20
中孚安全技术有限公司	15	15
杭州默安科技有限公司	9	9
河南信安世纪科技有限公司	8	8
北京远禾科技有限公司	8	8
山东九域信息技术有限公司	5	5
任子行网络技术股份有限公司	4	4
上海齐同信息科技有	4	4

限公司		
广州安亿信软件科技有限公司	4	4
汇安云（山东）信息科技有限公司	4	4
北京云科安信科技有限公司（Seraph 安全实验室）	4	4
苏州棱镜七彩信息科技有限公司	3	3
山东新潮信息技术有限公司	3	3
赛尔网络有限公司	2	2
北京威努特技术有限公司	2	2
上海市信息安全测评认证中心	1	1
中科国宏科技有限公司	1	1
上海天存信息技术有限公司	1	1
云南联创网安科技有限公司	1	1
内蒙古中叶信息技术有限责任公司	1	1
北京珞安科技有限责任公司	1	1
京数安（北京）科技有限公司	1	1
郑州埃文科技	1	1
河南灵创电子科技有限公司	1	1
信息产业信息安全测评中心	1	1
CNCERT 宁夏分中心	3	3

CNCERT 内蒙古分中心	1	1
个人	2330	2330
报送总计	26609	24061

本周漏洞按类型和厂商统计

本周，CNVD 收录了 246 个漏洞。WEB 应用 130 个，网络设备（交换机、路由器等网络端设备）60 个，应用程序 42 个，智能设备（物联网终端设备）10 个，操作系统 2 个，安全产品 2 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	130
网络设备（交换机、路由器等网络端设备）	60
应用程序	42
智能设备（物联网终端设备）	10
操作系统	2
安全产品	2

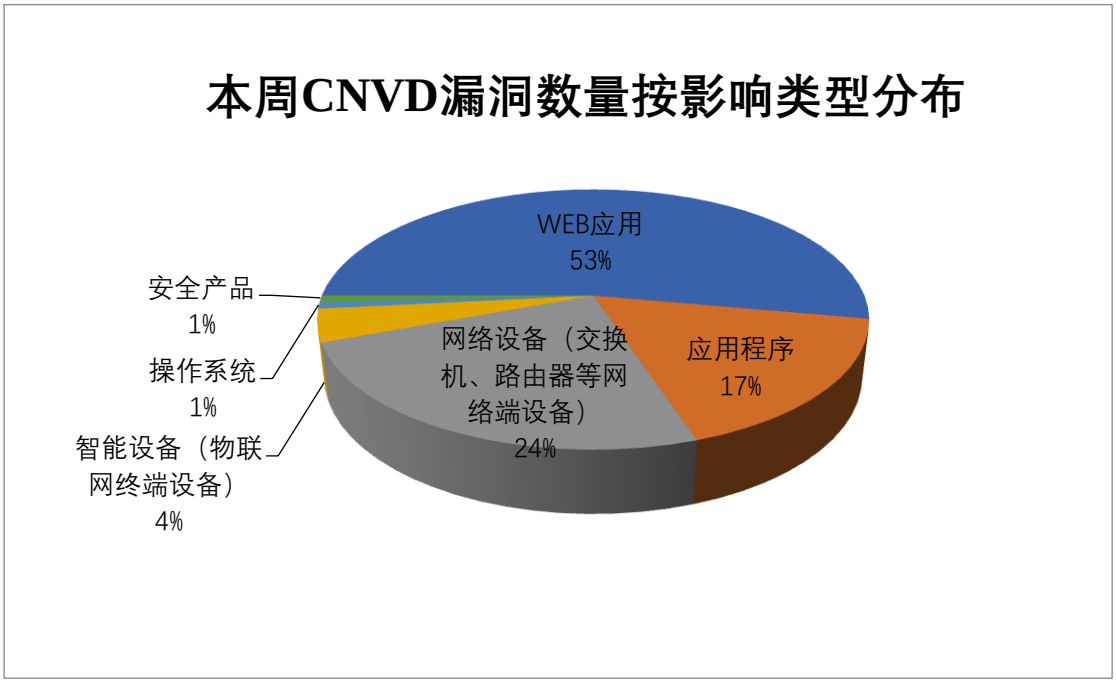

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 D-Link、Adobe、IBM 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	D-Link	21	9%
2	Adobe	12	5%
3	IBM	10	4%
4	Tenda	9	4%
5	LS ELECTRIC	8	3%
6	Simmeth System	6	2%
7	北京信安世纪科技股份有限公司	5	2%
8	北京网康科技有限公司	5	2%
9	TRENDnet	3	1%
10	其他	167	68%

本周行业漏洞收录情况

本周，CNVD 收录了 45 个电信行业漏洞，18 个移动互联网行业漏洞，10 个工控行业漏洞（如下图所示）。其中，“TRENDnet TEW-811DRU 命令注入漏洞（CNVD-2023-22721）、Tenda AX3 命令注入漏洞（CNVD-2023-21670）”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/

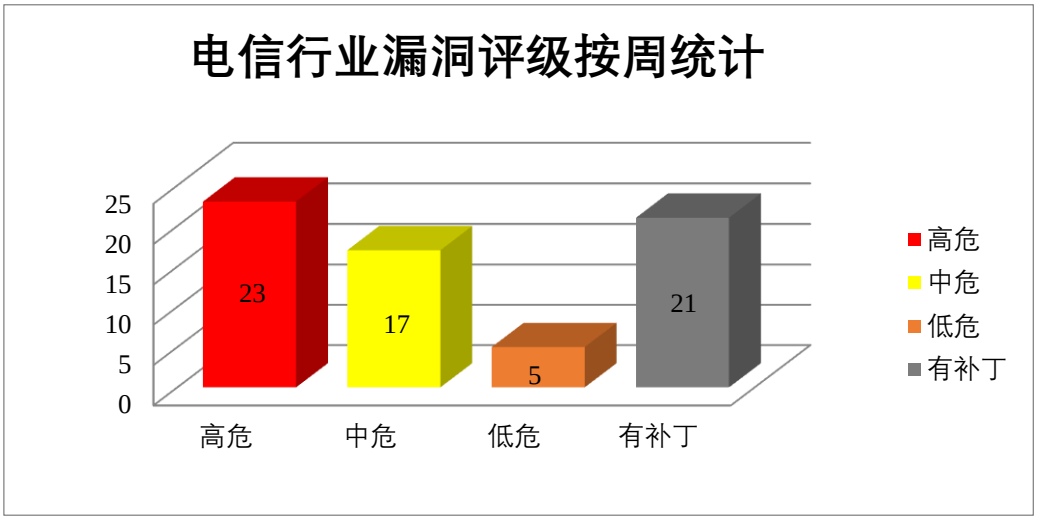

图 3 电信行业漏洞统计

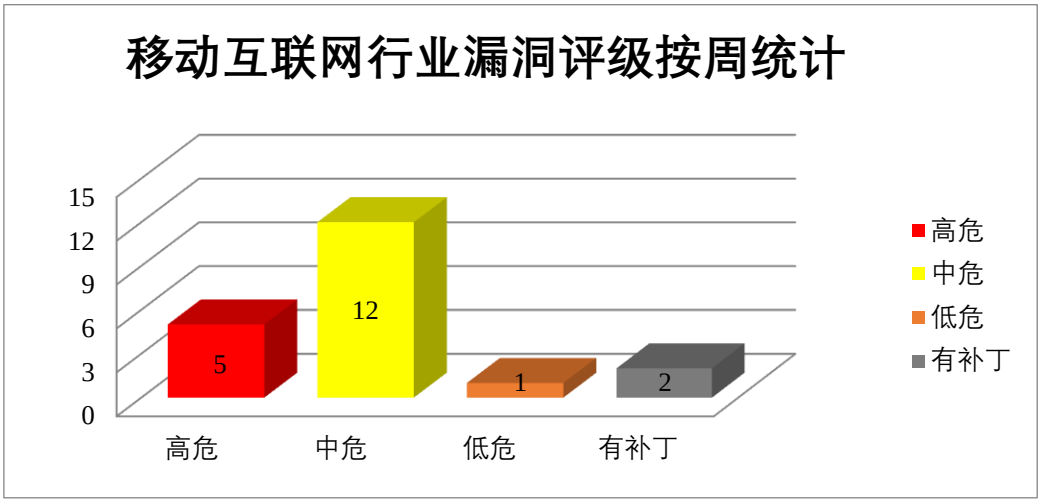

图 4 移动互联网行业漏洞统计

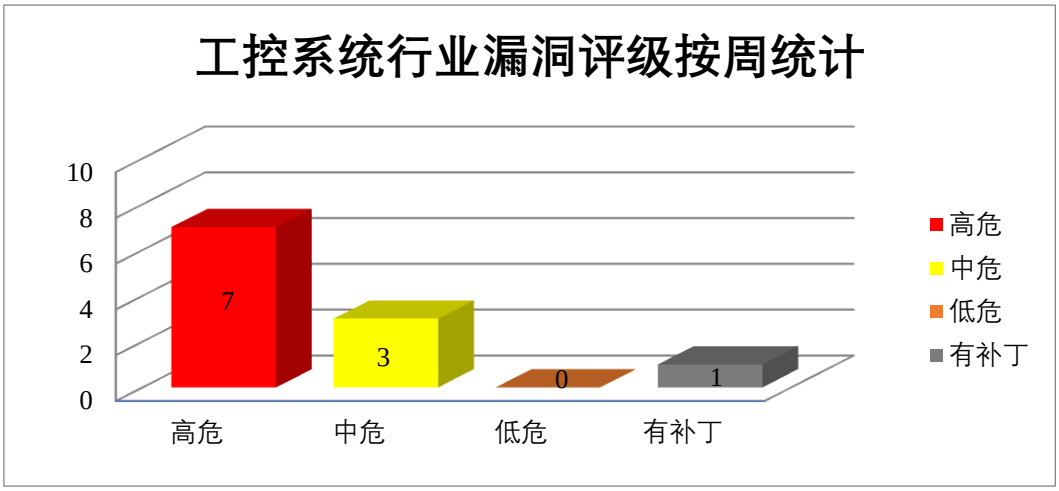

图 5 工控系统行业漏洞统计

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 Dimension 是美国奥多比（Adobe）公司的是一套 2D 和 3D 合成设计工具。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞在当前用户的上下文中执行任意代码。

CNVD 收录的相关漏洞包括：Adobe Dimension 输入验证错误漏洞（CNVD-2023-21649、CNVD-2023-21651）、Adobe Dimension 越界写入漏洞（CNVD-2023-21650）、Adobe Dimension 堆缓冲区溢出漏洞、Adobe Dimension 越界读取漏洞（CNVD-2023-21654、CNVD-2023-21658、CNVD-2023-21656、CNVD-2023-21657）。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-2023-21649

https://www.cnvd.org.cn/flaw/show/CNVD-2023-21650

https://www.cnvd.org.cn/flaw/show/CNVD-2023-21651

https://www.cnvd.org.cn/flaw/show/CNVD-2023-21654

https://www.cnvd.org.cn/flaw/show/CNVD-2023-21655

https://www.cnvd.org.cn/flaw/show/CNVD-2023-21656

https://www.cnvd.org.cn/flaw/show/CNVD-2023-21658

https://www.cnvd.org.cn/flaw/show/CNVD-2023-21657

2、D-Link 产品安全漏洞

D-Link DIR-2150 是 D-Link 公司的一个无线路由器设备。D-Link DWL-2600AP 是一款无线接入点设备。D-Link DIR-846 是一款无线路由器。D-Link DIR-825 是一款路由器。D-Link DIR-823G 是一款无线路由器。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特制数据包执行任意命令，在 root 上下文中执行代码等。

CNVD 收录的相关漏洞包括：D-Link DIR-2150 缓冲区溢出漏洞、D-Link DIR-2150 缓冲区溢出漏洞（CNVD-2023-21662、CNVD-2023-21663）、D-Link DIR-2150 操作系统命令注入漏洞（CNVD-2023-21660、CNVD-2023-21661）、D-Link DWL-2600AP 命令注入漏洞、D-Link DIR-846 命令注入漏洞（CNVD-2023-21666）、D-Link DIR-825 缓冲区溢出漏洞（CNVD-2023-21665）、D-Link DIR-823G 命令注入漏洞（CNVD-2023-21667）。其中，除“D-Link DWL-2600AP 命令注入漏洞”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-2023-21663

https://www.cnvd.org.cn/flaw/show/CNVD-2023-21662

https://www.cnvd.org.cn/flaw/show/CNVD-2023-21661

https://www.cnvd.org.cn/flaw/show/CNVD-2023-21660

https://www.cnvd.org.cn/flaw/show/CNVD-2023-21664

https://www.cnvd.org.cn/flaw/show/CNVD-2023-21666

https://www.cnvd.org.cn/flaw/show/CNVD-2023-21665

https://www.cnvd.org.cn/flaw/show/CNVD-2023-21667

3、IBM 产品安全漏洞

IBM Security Guardium Key ifecycle Manager 是管理通过集中化、精简化和自动化来进行加密密钥管理流程，以帮助保护加密数据和简化加密密钥管理。IBM Security Guardium 是一套提供数据保护功能的平台。该平台包括自定义 UI、报告管理和流线化的审计流程构建等功能。IBM Aspera 是一套基于 IBM FASP 协议构建的快速文件传输和流解决方案。IBM WebSphere Application Server（WAS）是一款应用服务器产品。该产品是 JavaEE 和 Web 服务应用程序的平台，也是 IBMWebSphere 软件平台的基础。

IBM Financial Transaction Manager 是一款金融事务管理器。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使用特制 URL 导致拒绝服务，执行非法 SQL 命令窃取数据库敏感数据，执行任意命令等。

CNVD 收录的相关漏洞包括：IBM Security Guardium Key Lifecycle Manager 未授权访问漏洞、IBM Security Guardium 信息泄露漏洞（CNVD-2023-20082）、IBM Security Guardium SQL 注入漏洞（CNVD-2023-20081）、IBM Aspera XML 外部实体注入漏洞、IBM Aspera Faspex SQL 注入漏洞、IBM Aspera 访问控制错误漏洞（CNVD-2023-20083）、IBM WebSphere Application Server 输入验证错误漏洞（CNVD-2023-20087）、IBM Financial Transaction Manager 目录遍历漏洞（CNVD-2023-20086）。其中，除“IBM Security Guardium Key Lifecycle Manager 未授权访问漏洞、IBM Security Guardium 信息泄露漏洞（CNVD-2023-20082）、IBM Security Guardium SQL 注入漏洞（CNVD-2023-20081）”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-2023-20078
https://www.cnvd.org.cn/flaw/show/CNVD-2023-20082
https://www.cnvd.org.cn/flaw/show/CNVD-2023-20081
https://www.cnvd.org.cn/flaw/show/CNVD-2023-20080
https://www.cnvd.org.cn/flaw/show/CNVD-2023-20079
https://www.cnvd.org.cn/flaw/show/CNVD-2023-20083
https://www.cnvd.org.cn/flaw/show/CNVD-2023-20087
https://www.cnvd.org.cn/flaw/show/CNVD-2023-20086

4、Tenda 产品安全漏洞

Tenda Ax3 是中国腾达（Tenda）公司的一款 Ax1800 千兆端口双频 Wifi 6 无线路由器。Tenda G103 是一款企业级 Ap 路由器。Tenda AC18 是一款路由器。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精心制作的包获取敏感信息，导致远程代码执行或者拒绝服务等。

CNVD 收录的相关漏洞包括：Tenda AX3 缓冲区溢出漏洞（CNVD-2023-21669）、Tenda G103 命令注入漏洞、Tenda AC18 缓冲区溢出漏洞（CNVD-2023-21673、CNVD-2023-21672、CNVD-2023-21671、CNVD-2023-21675、CNVD-2023-21674、CNVD-2023-21676）。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-2023-21669
https://www.cnvd.org.cn/flaw/show/CNVD-2023-21668
https://www.cnvd.org.cn/flaw/show/CNVD-2023-21673

https://www.cnvd.org.cn/flaw/show/CNVD-2023-21672

https://www.cnvd.org.cn/flaw/show/CNVD-2023-21671

https://www.cnvd.org.cn/flaw/show/CNVD-2023-21675

https://www.cnvd.org.cn/flaw/show/CNVD-2023-21674

https://www.cnvd.org.cn/flaw/show/CNVD-2023-21676

5、LS ELECTRIC XBC-DN32U 拒绝服务漏洞

LS ELECTRIC XBC-DN32U 是韩国 LS ELECTRIC 公司的一款 PLC 可编程逻辑控制器。本周，LS ELECTRIC XBC-DN32U 被披露存在拒绝服务漏洞。攻击者可利用该漏洞造成拒绝服务。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-2023-21683

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-2023-21652	Adobe Dimension 堆缓冲区溢出漏洞（CNVD-2023-21652）	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/apsb23-20.html
CNVD-2023-21653	Adobe Dimension 堆缓冲区溢出漏洞（CNVD-2023-21653）	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/apsb23-20.html
CNVD-2023-21659	D-Link DIR-882 缓冲区溢出漏洞（CNVD-2023-21659）	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-2023-20080	IBM Aspera XML 外部实体注入漏洞		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/6964694
CNVD-2023-21670	Tenda AX3 命令注入漏洞（CNVD-2023-21670）		厂商已发布了漏洞修复程序，请及时关注更新：https://www.tenda.com.cn/
CNVD-2023-22721	TRENDnet TEW-811DRU 命令注入漏洞（CNVD-2023-22721）		用户可参考如下厂商提供的安全补丁以修复该漏洞：https://www.trendnet.com/
CNVD-2023-21675	Tenda AC18 缓冲区溢出漏洞（CNVD-2023-21675）		厂商已发布了漏洞修复程序，请及时关注更新：

			https://www.tenda.cn
CNVD-2023-21667	D-Link DIR-823G 命令注入漏洞（CNVD-2023-21667）		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-2023-21665	D-Link DIR-825 缓冲区溢出漏洞（CNVD-2023-21665）		厂商已发布了漏洞修复程序，请及时关注更新：https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10314
CNVD-2023-21662	D-Link DIR-2150 缓冲区溢出漏洞（CNVD-2023-21662）		厂商已发布了漏洞修复程序，请及时关注更新：https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10304

小结：本周，Adobe 产品被披露存在多个漏洞，攻击者可利用漏洞在当前用户的上下文中执行任意代码。此外，D-Link、IBM、Tenda 等多款产品被披露存在多个漏洞，攻击者可利用漏洞通过精心制作的包获取敏感信息，导致远程代码执行或者拒绝服务，执行任意命令等。另外，LS ELECTRIC XBC-DN32U 被披露存在拒绝服务漏洞。攻击者可利用该漏洞造成拒绝服务。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、Eolinker SQL 注入漏洞

验证描述

Eolinker 是中国银云（Eolinker）公司的一个 API 管理解决方案。

Eolinker 存在 SQL 注入漏洞，该漏洞源于文件/plugin/getList 缺少对外部输入 SQL 语句的验证，攻击者可利用该漏洞获取数据库信息。

验证信息

POC 链接：https://c2.im5i.com/2022/11/09/XOvUn.pnghttps://c2.im5i.com/2022/11/09/XOq61.png

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2023-22681

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. WiFi 协议曝安全漏洞，影响 Linux、Android 和 iOS

来自美国东北大学和鲁汶大学的学者披露了一组 IEEE 802.11 Wi-Fi 协议标准的一个基础设计漏洞，影响到运行 Linux、FreeBSD、Android 和 iOS 的各种设备。

参考链接：https://www.freebuf.com/news/362195.html

2. QNAP 提醒客户尽快修补 NAS 设备中的 Linux Sudo 漏洞

中国台湾硬件供应商 QNAP 提醒客户保护其 Linux 供电的网络连接存储（NAS）设备免受 Sudo 权限升级漏洞的攻击。

参考链接：https://www.bleepingcomputer.com/news/security/qnap-warns-customers-to-patch-linux-sudo-flaw-in-nas-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