国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2023 年 06 月 26 日-2023 年 07 月 02 日　　2023 年第 26 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 450 个，其中高危漏洞 220 个、中危漏洞 205 个、低危漏洞 25 个。漏洞平均分值为 6.55。本周收录的漏洞中，涉及 0day 漏洞 371 个（占 82%），其中互联网上出现“TOTOLINK A7100RU 命令注入漏洞（CNVD-2023-51676）、D-Link DIR-600 缓冲区溢出漏洞”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 7988 个，与上周（9819 个）环比减少 19%。

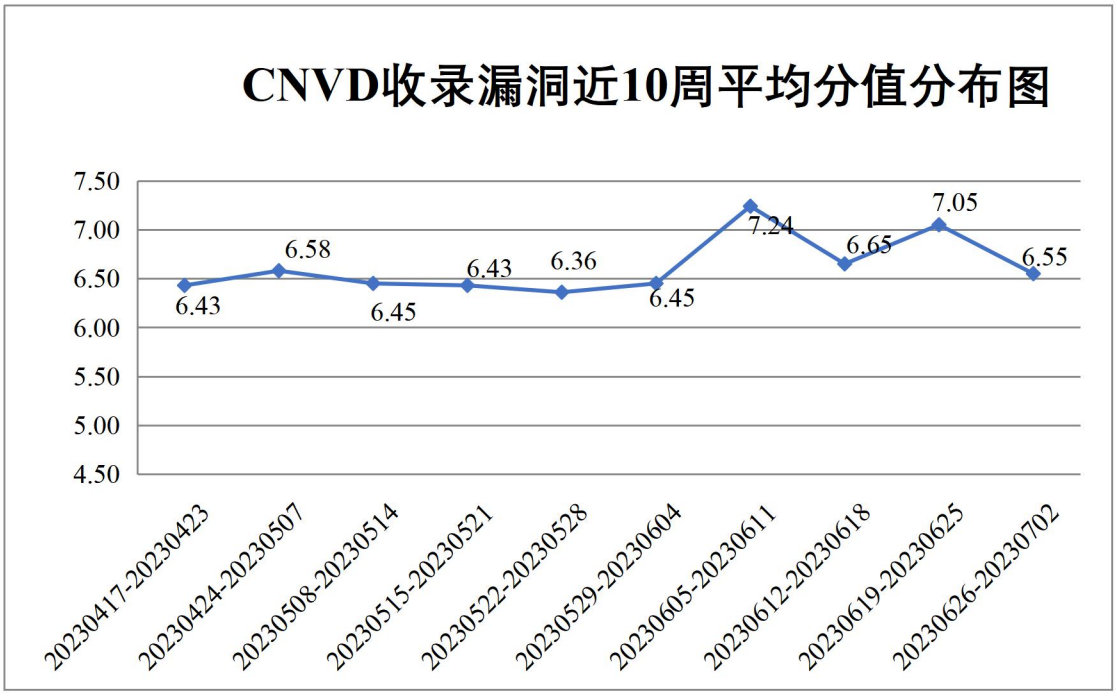

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 42 起，向基础电

信企业通报漏洞事件 16 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 1129 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 222 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 53 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：

珠海港信息技术股份有限公司、重庆森鑫炬科技有限公司、重庆泛普软件有限公司、中企动力科技股份有限公司、正方软件股份有限公司、浙江万朋数智科技股份有限公司、浙江美术传媒拍卖有限公司、掌如科技服务有限公司、长安马自达汽车有限公司、云南恩捷新材料股份有限公司、友讯电子设备（上海）有限公司、用友网络科技股份有限公司、永中软件股份有限公司、义乌中国小商品城大数据有限公司、研华科技（中国）有限公司、芜湖安得智联科技有限公司、无锡信捷电气股份有限公司、温州莱泽气动科技有限公司、统信软件技术有限公司、天维尔信息科技股份有限公司、天津天堰科技股份有限公司、天津市康婷生物工程集团有限公司、天津生态城投资开发有限公司、腾讯安全应急响应中心、特斯拉（上海）有限公司、台达集团、拓水科技（张家港）有限公司、速达软件技术（广州）有限公司、苏州蓝鹤信息技术有限公司、神州数码集团股份有限公司、深圳坐标软件集团有限公司、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、深圳市校鸽科技有限公司、深圳市网域科技股份有限公司、深圳市拓普泰尔科技有限公司、深圳市联软科技股份有限公司、深圳市捷顺科技实业股份有限公司、深圳市吉祥腾达科技有限公司、深圳市和为顺网络技术有限公司、深圳市海融易通电子有限公司、深圳市必联电子有限公司、深圳市爱八方健康有限公司、深圳开源互联网安全技术有限公司、深圳华视美达信息技术有限公司、深圳邦健生物医疗设备股份有限公司、上海卓卓网络科技有限公司、上海装盟信息科技有限公司、上海英立视数字科技有限公司、上海尚尚健康管理咨询有限公司、上海纽盾科技股份有限公司、上海明厦物联网科技有限公司、上海居亦科技发展有限公司、上海寰创通信科技股份有限公司、上海酆泽信息技术有限公司、上海斐讯数据通信技术有限公司、上海泛微网络科技股份有限公司、上海繁易信息科技股份有限公司、上海贝锐信息科技股份有限公司、上海宝尊电子商务有限公司、上海百胜软件股份有限公司、熵基科技股份有限公司、商派软件有限公司、山东京帝软件有限公司、厦门四信通信科技有限公司、荣万家生活服务股份有限公司、青岛东软载波智能电子有限公司、千申医疗科技（上海）有限公司、普元信息技术股份有限公司、南阳仲景百信医药科技有限公司、南京科远智慧科技集团股份有限公司、南京访客乐网络科技有限公司、美味不用等（上海）信息科技股份有限公司、迈普通信技术股份有限公司、蚂蚁科技集团股份有限公司、辽源市国安公共自行车有限公司、金锋食品科技（苏州）有限公司、江西志浩电子科技有限公司、济南有人物联网技术有限公司、济南驰骋信息技术有限公司、吉翁电子（深圳）有限公司、惠普贸易（上海）有限

公司、湖南润安危物联科技发展有限公司、湖北源尖软件科技有限公司、红门智能科技股份有限公司、河南众寻网信息技术有限公司、杭州叙简科技股份有限公司、杭州雄伟科技开发股份有限公司、杭州雄迈信息技术有限公司（XMSRC）、杭州九麒科技有限公司、杭州海康威视数字技术股份有限公司、哈尔滨新中新电子股份有限公司、广州协众软件科技有限公司、广州图创计算机软件开发有限公司、广州同聚成电子科技有限公司、广州添富信息科技有限责任公司、广州市人易软件技术有限公司、广东申义实业投资有限公司、福州翔升软件开发有限公司、方心科技股份有限公司、东易日盛家居装饰集团股份有限公司、点都互联科技有限公司、道尔智控科技股份有限公司、大农科技股份有限公司、大连万达集团股份有限公司、大连菲尔科技有限公司、成都星锐蓝海网络科技有限公司、成都网旗云科信息技术有限公司、成都任我行软件股份有限公司、成都华嘉利科技有限公司、成都创新互联科技有限公司、禅道软件（青岛）有限公司、北京中科华博科技有限公司、北京易普行科技有限公司、北京星网锐捷网络技术有限公司、北京信诺瑞得软件系统有限公司、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、北京润乾信息系统技术有限公司、北京启明星辰信息安全技术有限公司、北京灵州网络技术有限公司、北京久其软件股份有限公司、北京鸿益达科技有限公司、北京宏景世纪软件股份有限公司、北京百卓网络技术有限公司、北京奥博威斯科技有限公司、保定市公共交通有限公司、傲拓科技股份有限公司、安徽旭帆信息科技有限公司、安徽皖通邮电股份有限公司、爱能盛世（广东）教育科技控股股份有限公司、阿里巴巴集团安全应急响应中心、TRENDnet、Jeeplus 和 DzzOffice。

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，北京天融信网络安全技术有限公司、新华三技术有限公司、北京神州绿盟科技有限公司、深信服科技股份有限公司、安天科技集团股份有限公司等单位报送公开收集的漏洞数量较多。河南信安世纪科技有限公司、快页信息技术有限公司、杭州美创科技有限公司、内蒙古中叶信息技术有限责任公司、奇安星城网络安全运营服务（长沙）有限公司、河南东方云盾信息技术有限公司、安徽锋刃信息科技有限公司、联想集团、内蒙古洞明科技有限公司、重庆电信系统集成有限公司、贵州多彩网安科技有限公司、赛尔网络有限公司、杭州默安科技有限公司、信息产业信息安全测评中心、江苏极元信息技术有限公司、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、河南省鼎信信息安全等级测评有限公司、北京云科安信科技有限公司（Seraph 安全实验室）、河北镌远网络科技有限公司、深圳建安润星安全技术有限公司、内蒙古奥创网安科技有限公司、中能融合智慧科技有限公司、亚信科技（成都）有限公司、山东正中信息技术股份有限公司、超聚变数字技术有限公司、北京墨云科技有限公司、山石网科通信技术股份有限公司、北京珞安科技有限责任公司、河南灵创电

子科技有限公司及其他个人白帽子向 CNVD 提交了 7988 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 5973 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）	3316	3316
奇安信网神（补天平台）	1408	1408
北京天融信网络安全技术有限公司	925	2
上海交大	728	728
新华三技术有限公司	559	0
北京神州绿盟科技有限公司	531	3
三六零数字安全科技集团有限公司	521	521
深信服科技股份有限公司	409	1
安天科技集团股份有限公司	400	0
北京数字观星科技有限公司	165	0
北京长亭科技有限公司	84	0
北京启明星辰信息安全技术有限公司	78	1
天津市国瑞数码安全系统股份有限公司	59	0
远江盛邦（北京）网络安全科技股份有限公司	57	57
杭州迪普科技股份有限公司	14	0
杭州安恒信息技术股份有限公司	10	10

阿里云计算有限公司	4	4
浙江大华技术股份有限公司	2	2
北京知道创宇信息技术有限公司	2	1
北京智游网安科技有限公司	1	1
河南信安世纪科技有限公司	100	100
快页信息技术有限公司	51	51
杭州美创科技有限公司	47	47
内蒙古中叶信息技术有限责任公司	38	38
奇安星城网络安全运营服务（长沙）有限公司	37	37
河南东方云盾信息技术有限公司	29	29
安徽锋刃信息科技有限公司	24	24
联想集团	17	17
内蒙古洞明科技有限公司	8	8
重庆电信系统集成有限公司	7	7
贵州多彩网安科技有限公司	7	7
赛尔网络有限公司	6	6
杭州默安科技有限公司	4	4
信息产业信息安全测评中心	4	4
江苏极元信息技术有	3	3

限公司		
北京山石网科信息技术有限公司	3	3
博智安全科技股份有限公司	3	3
河南省鼎信信息安全等级测评有限公司	3	3
北京云科安信科技有限公司（Seraph 安全实验室）	2	2
河北锎远网络科技有限公司	2	2
深圳建安润星安全技术有限公司	2	2
内蒙古奥创网安科技有限公司	2	2
中能融合智慧科技有限公司	2	2
亚信科技（成都）有限公司	1	1
山东正中信息技术股份有限公司	1	1
超聚变数字技术有限公司	1	1
北京墨云科技有限公司	1	1
山石网科通信技术股份有限公司	1	1
北京珞安科技有限责任公司	1	1
河南灵创电子科技有限公司	1	1
CNCERT 河北分中心	3	3
CNCERT 宁夏分中心	2	2
CNCERT 广西分中心	1	1

个人	1519	1519
报送总计	11206	7988

本周漏洞按类型和厂商统计

本周，CNVD 收录了 450 个漏洞。WEB 应用 257 个，应用程序 87 个，网络设备（交换机、路由器等网络端设备）72 个，操作系统 19 个，智能设备（物联网终端设备）13 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	257
应用程序	87
网络设备（交换机、路由器等网络端设备）	72
操作系统	19
智能设备（物联网终端设备）	13
安全产品	2

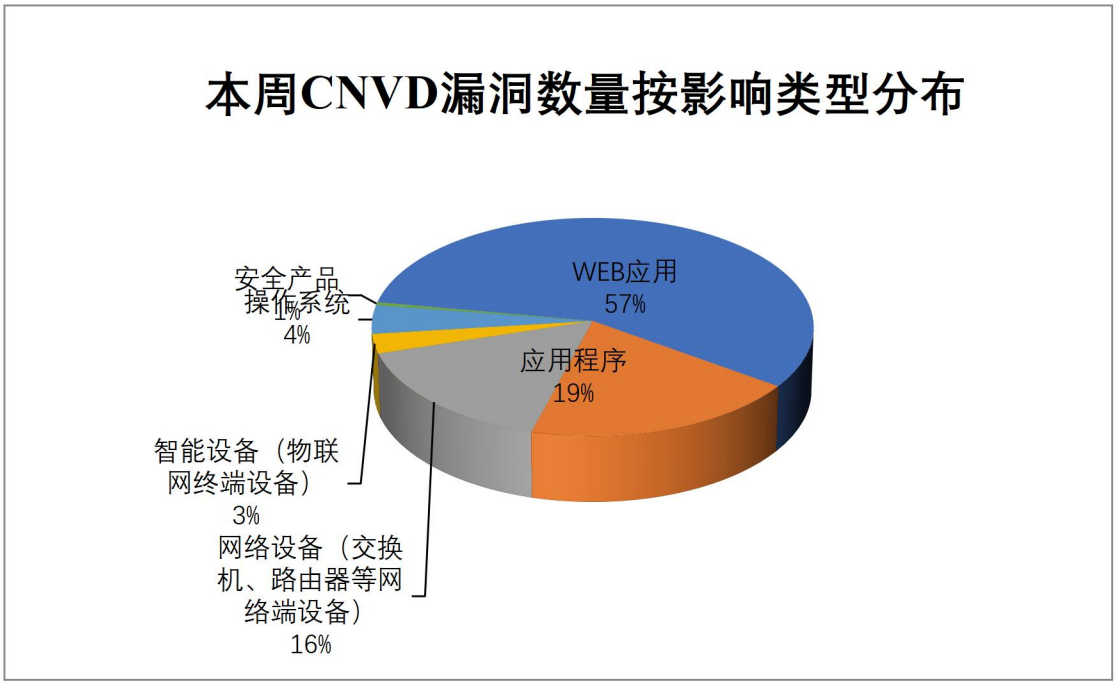

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Adobe、Microsoft、Linux 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	13	3%
2	Microsoft	12	2%
3	Linux	11	2%
4	IBM	11	2%
5	厦门四信通信科技有限公司	9	2%
6	北京网康科技有限公司	7	2%
7	H3C	7	2%
8	Google	7	2%
9	北京百卓网络技术有限公司	7	2%
10	其他	366	81%

本周行业漏洞收录情况

本周，CNVD 收录了 46 个电信行业漏洞，44 个移动互联网行业漏洞，7 个工控行业漏洞（如下图所示）。其中，“H3C Magic R300 堆栈溢出漏洞、Google Android 缓冲区溢出漏洞（CNVD-2023-52817）”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/

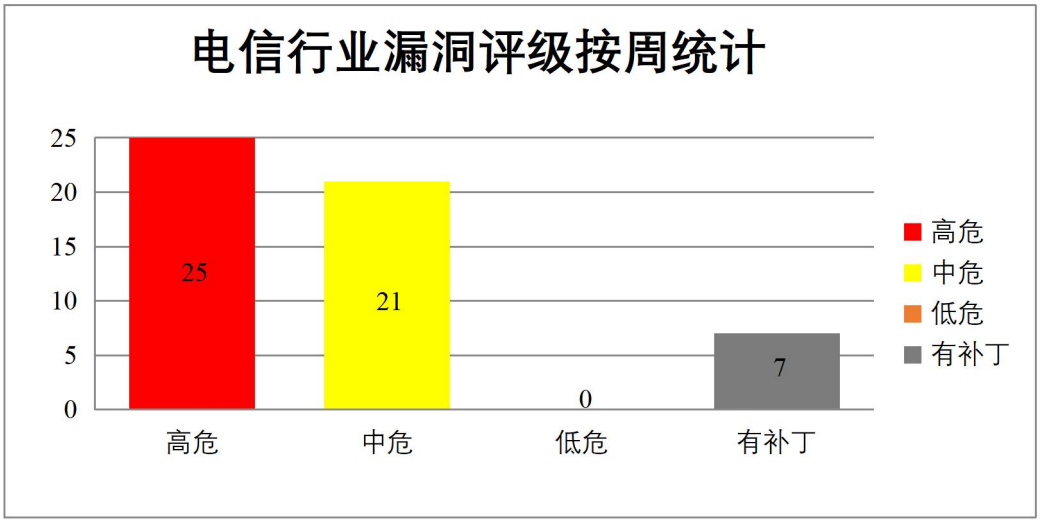

图 3 电信行业漏洞统计

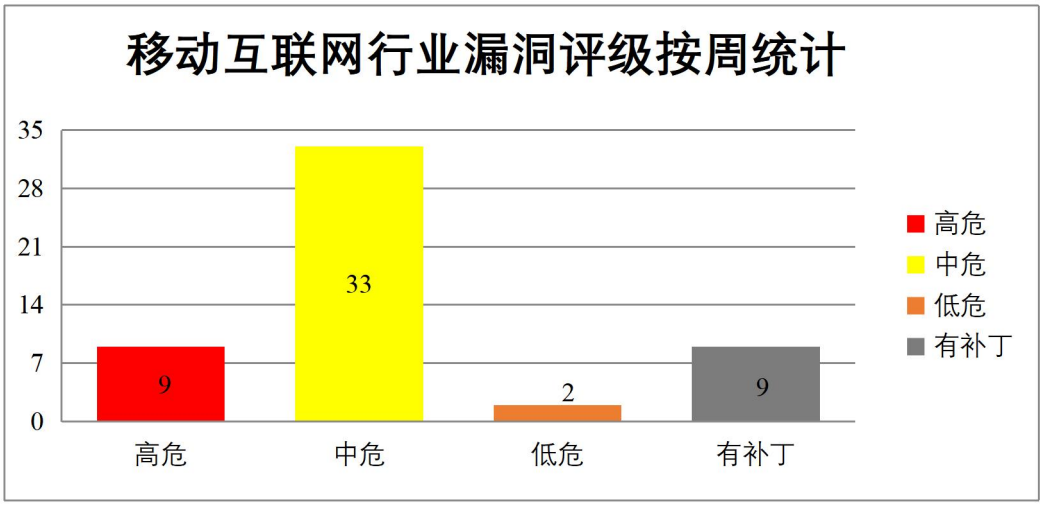

图 4 移动互联网行业漏洞统计

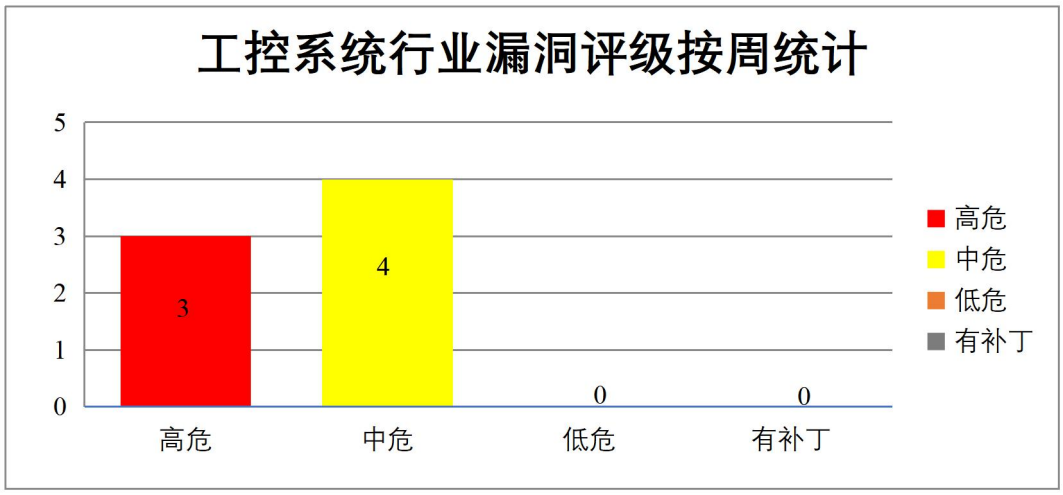

图 5 工控系统行业漏洞统计

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 Acrobat Reader 是美国奥多比（Adobe）公司的一款 PDF 查看器。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，导致敏感内存泄露。

CNVD 收录的相关漏洞包括：Adobe Acrobat and Reader 输入验证错误漏洞、Adobe Acrobat and Reader 释放后使用漏洞、Adobe Acrobat and Reader 越界写入漏洞（CNVD-2023-51680、CNVD-2023-51683）、Adobe Acrobat and Reader 越界读取漏洞、Adobe Acrobat and Reader 缓冲区溢出漏洞（CNVD-2023-51679、CNVD-2023-51685、CNVD-2023-51684）。其中，除“Adobe Acrobat and Reader 越界读取漏洞”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-2023-51682
https://www.cnvd.org.cn/flaw/show/CNVD-2023-51681
https://www.cnvd.org.cn/flaw/show/CNVD-2023-51680
https://www.cnvd.org.cn/flaw/show/CNVD-2023-51679
https://www.cnvd.org.cn/flaw/show/CNVD-2023-51686
https://www.cnvd.org.cn/flaw/show/CNVD-2023-51685
https://www.cnvd.org.cn/flaw/show/CNVD-2023-51684
https://www.cnvd.org.cn/flaw/show/CNVD-2023-51683

2、IBM 产品安全漏洞

IBM PowerVM Hypervisor 是美国国际商业机器（IBM）公司的一个应用软件。提供了一个安全且可扩展的虚拟化环境，这些应用程序基于 Power Systems 平台的高级 RAS 功能和领先性能而构建。IBM Security Directory Suite 是一个可扩展的、基于标准的身份平台，可简化身份和目录管理。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，攻击者可利用漏洞通过发送特制请求在系统上执行任意命令，在获取对 HMC 的业务访问权限后获取敏感信息，导致拒绝服务等。

CNVD 收录的相关漏洞包括：IBM Security Directory Suite VA 操作系统命令注入漏洞、IBM Security Directory Suite VA 信息泄露漏洞（CNVD-2023-51453、CNVD-2023-51456、CNVD-2023-51455）、IBM PowerVM Hypervisor 信息泄露漏洞、IBM Security Directory Suite VA 资源管理错误漏洞、IBM Security Directory Suite VA 文件上传漏洞、IBM Sterling Partner Engagement Manager 跨站脚本漏洞（CNVD-2023-51460）。其中，“IBM Security Directory Suite VA 操作系统命令注入漏洞、IBM Security Directory Suite VA 资源管理错误漏洞、IBM Security Directory Suite VA 文件上传漏洞、IBM Security Directory Suite VA 信息泄露漏洞（CNVD-2023-51455）”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-2023-51454
https://www.cnvd.org.cn/flaw/show/CNVD-2023-51453
https://www.cnvd.org.cn/flaw/show/CNVD-2023-51452
https://www.cnvd.org.cn/flaw/show/CNVD-2023-51458
https://www.cnvd.org.cn/flaw/show/CNVD-2023-51457
https://www.cnvd.org.cn/flaw/show/CNVD-2023-51456
https://www.cnvd.org.cn/flaw/show/CNVD-2023-51455
https://www.cnvd.org.cn/flaw/show/CNVD-2023-51460

3、Linux 产品安全漏洞

Linux kernel 是美国 Linux 基金会的开源操作系统 Linux 所使用的内核。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拒绝服务或权限升级，任意代码执行等。

CNVD 收录的相关漏洞包括：Linux kernel 缓冲区溢出漏洞（CNVD-2023-51380、CNVD-2023-51379、CNVD-2023-51387）、Linux kernel 权限提升漏洞（CNVD-2023-51385）、Linux Kernel 资源管理错误漏洞（CNVD-2023-51384、CNVD-2023-51381）、Linux kernel 信息泄露漏洞（CNVD-2023-51386）、Linux kernel 拒绝服务漏洞（CNVD-2023-51389）。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-2023-51381
https://www.cnvd.org.cn/flaw/show/CNVD-2023-51380
https://www.cnvd.org.cn/flaw/show/CNVD-2023-51379
https://www.cnvd.org.cn/flaw/show/CNVD-2023-51385
https://www.cnvd.org.cn/flaw/show/CNVD-2023-51384
https://www.cnvd.org.cn/flaw/show/CNVD-2023-51387
https://www.cnvd.org.cn/flaw/show/CNVD-2023-51386
https://www.cnvd.org.cn/flaw/show/CNVD-2023-51389

4、 Microsoft 产品安全漏洞

Microsoft Exchange Server 是美国微软（Microsoft）公司的一套电子邮件服务程序。它提供邮件存取、储存、转发，语音邮件，邮件过滤筛选等功能。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，在系统上获得提升的权限等。

CNVD 收录的相关漏洞包括：Microsoft Exchange Server 远程代码执行漏洞（CNVD-2023-51368、CNVD-2023-51369、CNVD-2023-51370、CNVD-2023-51371、CNVD-2023-51372）、Microsoft Exchange Server 权限提升漏洞（CNVD-2023-51374、CNVD-2023-51375、CNVD-2023-51378）。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-2023-51368
https://www.cnvd.org.cn/flaw/show/CNVD-2023-51369
https://www.cnvd.org.cn/flaw/show/CNVD-2023-51370
https://www.cnvd.org.cn/flaw/show/CNVD-2023-51371
https://www.cnvd.org.cn/flaw/show/CNVD-2023-51372
https://www.cnvd.org.cn/flaw/show/CNVD-2023-51374
https://www.cnvd.org.cn/flaw/show/CNVD-2023-51375

https://www.cnvd.org.cn/flaw/show/CNVD-2023-51378

5、Tenda G103 命令注入漏洞（CNVD-2023-52857）

Tenda G103 是中国腾达（Tenda）公司的一个专为家庭、SOHO 用户设计的 GPON 光纤接入设备。本周，Tenda G103 被披露存在命令注入漏洞。攻击者可利用该漏洞注入获取 shell 权限的命令。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-2023-52857

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-2023-51377	Microsoft Exchange Server 欺骗漏洞（CNVD-2023-51377）	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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-21762
CNVD-2023-51675	Huawei BiSheng-WNM FW 拒绝服务漏洞（CNVD-2023-51675）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.huawei.com/en/psirt/security-advisories/2023/huawei-sa-moivihp-2f201af9-en
CNVD-2023-51677	TOTOLINK CP900 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://totolink.cn/home/menu/detail.html?menu_listtpl=download&id=51&ids=36
CNVD-2023-52053	H3C Magic R300 堆栈溢出漏洞（CNVD-2023-52053）	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.h3c.com/
CNVD-2023-52054	H3C Magic R300 堆栈溢出漏洞（CNVD-2023-52054）	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.h3c.com/
CNVD-2023-52698	Mozilla Firefox 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://www.mozilla.org/security/advisories/mfsa2023-01/
CNVD-2023-52697	Mozilla Firefox 缓冲区溢出漏洞（CNVD-2023-52697）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.mozilla.org/en-US/security/advisories/mfsa2023-05/

CNVD-2023-52699	Apache Sling 输入验证错误漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://lists.apache.org/thread/sws7z50x47gv0c38q4kx6ktqrvrrg1pm
CNVD-2023-52816	Google Android 越界写入漏洞（CNVD-2023-52816）	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/2023-06-01
CNVD-2023-52831	Jellyfin 存在 SSRF 漏洞（CNVD-2023-52831）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/jellyfin/jellyfin/releases/tag/v10.8.9

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，导致敏感内存泄露。此外，IBM、Linux、Microsoft 等多款产品被披露存在多个漏洞，攻击者可利用漏洞通过发送特制请求在系统上执行任意命令，获取敏感信息，导致拒绝服务等。另外，Tenda G103 被披露存在命令注入漏洞。攻击者可利用该漏洞注入获取 shell 权限的命令。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 DIR-600 缓冲区溢出漏洞

验证描述

D-Link DIR-600 是中国友讯（D-Link）公司的一款无线路由器。

D-Link DIR-600 2.18 版本存在缓冲区溢出漏洞，该漏洞源于文件 gena.cgi 在处理未受信任的输入时出现边界错误，攻击者可利用该漏洞在系统上执行任意代码或者导致拒绝服务攻击。

验证信息

POC 链接：https://github.com/naihsin/IoT/blob/main/D-Link/DIR-600/overflow/README.md

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2023-52856

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. WordPress 社交登录插件曝出漏洞，用户账户信息遭泄露

The Hacker News 网站消息，miniOrange 的 WordPress 社交登录和注册插件中出现了一个安全漏洞，该漏洞可能使潜在网络攻击者登录用户帐户。

参考链接：https://thehackernews.com/2023/06/critical-security-flaw-in-social-login.html

2. SQL 注入缺陷使 Gentoo Soko 遭受远程代码执行

Gentoo Soko 中已披露多个 SQL 注入漏洞，这些漏洞可能导致在易受攻击的系统上进行远程代码执行。

参考链接：https://thehackernews.com/2023/06/critical-sql-injection-flaws-expose.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