国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2022 年 06 月 06 日-2022 年 06 月 12 日 **2022 年第 23 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 542 个，其中高危漏洞 169 个、中危漏洞 292 个、低危漏洞 81 个。漏洞平均分值为 5.57。本周收录的漏洞中，涉及 0day 漏洞 396 个（占 73%），其中互联网上出现“Student Grading System SQL 注入漏洞（CNVD-2022-44234）、Purchase Order Management System 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事件型漏洞总数 42217 个，与上周（4943 个）环比增加 754%。

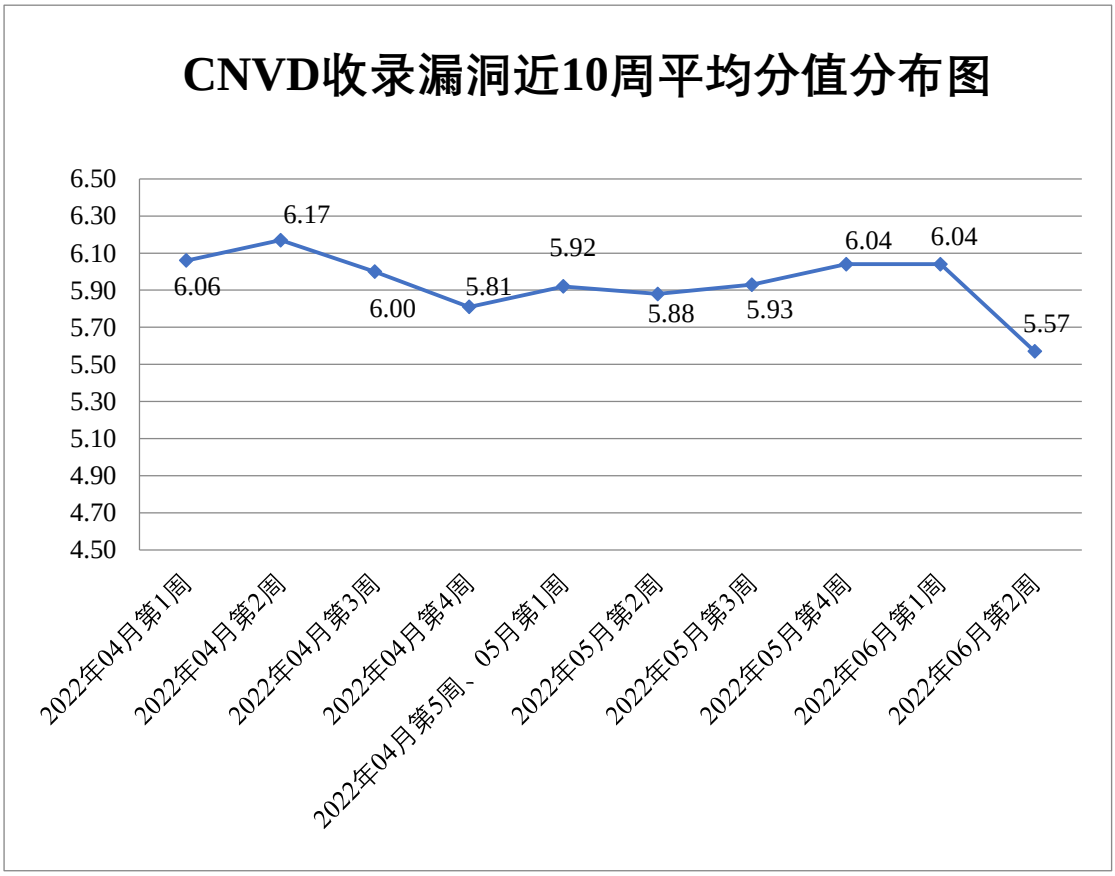

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 34 起，向基础电信企业通报漏洞事件 27 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 206 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 61 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 135 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：

紫光云技术有限公司、珠海经济特区伟思有限公司、重庆远秋科技有限公司、智互联（深圳）科技有限公司、浙江宇视科技有限公司、浙江大华技术股份有限公司、远景能源有限公司、友讯电子设备（上海）有限公司、永中软件股份有限公司、兄弟（中国）商业有限公司、新开普电子股份有限公司、新疆金风科技股份有限公司、西安佰联网络技术有限公司、武汉金水来科技发展股份有限公司、微软（中国）有限公司、微宏软件技术（杭州）有限公司、天津市集翔企商科技有限公司、天津神州浩天科技有限公司、腾智信息技术有限公司、苏州科达科技股份有限公司、四平市九州易通科技有限公司、四川迅睿云软件开发有限公司、思科系统（中国）网络技术有限公司、视联动力信息技术股份有限公司、沈阳普惠万通科技有限公司、深圳智慧光迅信息技术有限公司、深圳智慧光迅信息技术有限公、深圳市圆梦云科技有限公司、深圳市同为数码科技股份有限公司、深圳市美科星通信技术有限公司、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、上海云翌通信科技有限公司、上海凯京信达科技集团有限公司、上海顶想信息科技有限公司、上海大易云计算有限公司、上海博达数据通信有限公司、山东科德电子有限公司、厦门四信通信科技有限公司、厦门科拓通讯技术股份有限公司、锐捷网络股份有限公司、鹏为软件股份有限公司、宁波市鄞州英赛特软件有限公司、南通艾睦网络科技有限公司、南京九则软件科技有限公司、茉柏枘（上海）软件科技有限公司、明腾网络股份有限公司、莱克斯科技（北京）有限公司、昆明云涛科技有限公司、金科地产集团股份有限公司、江苏易索电子科技股份有限公司、江苏赛达电子科技有限公司、嘉兴市米洛网络科技有限公司、佳能（中国）有限公司、吉翁电子（深圳）有限公司、杭州迪普科技股份有限公司、贵州源溯科技有限公司、广州中望龙腾软件股份有限公司、广州易全信息科技有限公司、广州南方测绘科技股份有限公司广州分公司、广州航诚信息科技有限公司、广州扁担互联科技有限公司、广州安网通信技术有限公司、广西通济科技有限公司、广东顺景软件科技有限公司、广东堡塔安全技术有限公司、富士胶片商业创新（中国）有限公司、福建福昕软件开发股份有限公司、佛山市杜特软件科技有限公司、成都青软青之软件有限公司、北京中易银合科技有限公司、北京中景合天科技有限公司、北京易勤信息技术有限公司、北京星网锐捷网络技术有限公司、北京

微瑞集智科技有限公司、北京网御星云信息技术有限公司、北京网动网络科技股份有限公司、北京拓尔思信息技术股份有限公司、北京趋势威尔网络技术有限公司、北京良精志诚科技有限责任公司、北京蓝雁科技有限公司、北京酷我科技有限公司、北京九思协同软件有限公司、北京金钥匙凯丽科技发展有限公司、北京火星高科数字科技有限公司、北京工信信息技术有限公司、北京辰信领创信息技术有限公司、北京百卓网络技术有限公司、北大方正集团有限公司、《中国学术期刊（光盘版）》电子杂志社有限公司、帝国软件、站帮主 CMS、zzzcms、Zebra Technologies、VMware, Inc.、The Apache Software Foundation、Pisces Technology Co., Ltd.、OPENSSL、NETGEAR、Jeeplus、Glyph & Cog, LLC、EL-ADMIN、BotFactory Inc.、Belkin International, Inc.和 Adobe。

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，杭州安恒信息技术股份有限公司、北京神州绿盟科技有限公司、深信服科技股份有限公司、新华三技术有限公司、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。北京华顺信安科技有限公司、上海纽盾科技股份有限公司、星云博创科技有限公司、重庆都会信息科技、河南东方云盾信息技术有限公司、江苏保旺达软件技术有限公司、北方实验室（沈阳）股份有限公司、快页信息技术有限公司、杭州默安科技有限公司、长春嘉诚信息技术股份有限公司、武汉安域信息安全技术有限公司、山东云天安全技术有限公司、北京云科安信科技有限公司（Seraph 安全实验室）、中国烟草总公司湖北省公司、郑州向心力通信技术股份有限公司、河南信安世纪科技有限公司、山谷网安科技股份有限公司、河南省鼎信信息安全等级测评有限公司、山石网科通信技术股份有限公司、广东唯顶信息科技股份有限公司、江苏天竞云合数据技术有限公司、上海天存信息技术有限公司、北京升鑫网络科技有限公司、江苏国泰新点软件有限公司、贵州泰若数字科技有限公司、北京边界无限科技有限公司、北京机沃科技有限公司、任子行网络技术股份有限公司及其他个人白帽子向 CNVD 提交了 42217 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）、上海交大、奇安信网神（补天平台）和三六零数字安全科技集团有限公司向 CNVD 共享的白帽子报送的 39872 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
三六零数字安全科技集团有限公司	34753	34753
斗象科技（漏洞盒子）	3162	3162
奇安信网神（补天平台）	1845	1845

杭州安恒信息技术股份有限公司	582	431
北京神州绿盟科技有限公司	504	2
深信服科技股份有限公司	409	0
新华三技术有限公司	334	0
安天科技集团股份有限公司	229	0
上海交大	112	112
厦门服云信息科技有限公司	157	0
恒安嘉新（北京)科技股份公司	102	0
西安四叶草信息技术有限公司	91	91
天津市国瑞数码安全系统股份有限公司	59	0
京东科技信息技术有限公司	57	0
北京启明星辰信息安全技术有限公司	54	0
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	24	0
卫士通信息产业股份有限公司	19	5
杭州迪普科技股份有限公司	15	0
北京天融信网络安全技术有限公司	10	10
内蒙古云科数据服务股份有限公司	7	7
南京联成科技发展股	2	2

份有限公司		
北京华顺信安科技有限公司	154	5
墨菲未来科技（北京）有限公司	34	0
上海纽盾科技股份有限公司	33	33
星云博创科技有限公司	21	21
重庆都会信息科技	14	14
河南东方云盾信息技术有限公司	8	8
江苏保旺达软件技术有限公司	6	6
北方实验室（沈阳）股份有限公司	4	4
快页信息技术有限公司	4	4
杭州默安科技有限公司	4	4
长春嘉诚信息技术股份有限公司	3	3
武汉安域信息安全技术有限公司	3	3
山东云天安全技术有限公司	3	3
北京云科安信科技有限公司（Seraph 安全实验室）	2	2
中国烟草总公司湖北省公司	2	2
郑州向心力通信技术股份有限公司	2	2
河南信安世纪科技有限公司	2	2

山谷网安科技股份有限公司	1	1
河南省鼎信信息安全等级测评有限公司	1	1
山石网科通信技术股份有限公司	1	1
广东唯顶信息科技股份有限公司	1	1
江苏天竞云合数据技术有限公司	1	1
上海天存信息技术有限公司	1	1
北京升鑫网络科技有限公司	1	1
江苏国泰新点软件有限公司	1	1
贵州泰若数字科技有限公司	1	1
北京边界无限科技有限公司	1	1
北京机沃科技有限公司	1	1
任子行网络技术股份有限公司	1	1
CNCERT 河北分中心	6	6
CNCERT 四川分中心	4	4
个人	1659	1659
报送总计	44536	42217

本周漏洞按类型和厂商统计

本周，CNVD 收录了 542 个漏洞。WEB 应用 248 个，应用程序 111 个，操作系统 70 个，网络设备（交换机、路由器等网络端设备）64 个，安全产品 20 个，智能设备（物联网终端设备）16 个，数据库 13 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	248
应用程序	111
操作系统	70
网络设备（交换机、路由器等网络端设备）	64
安全产品	20
智能设备（物联网终端设备）	16
数据库	13

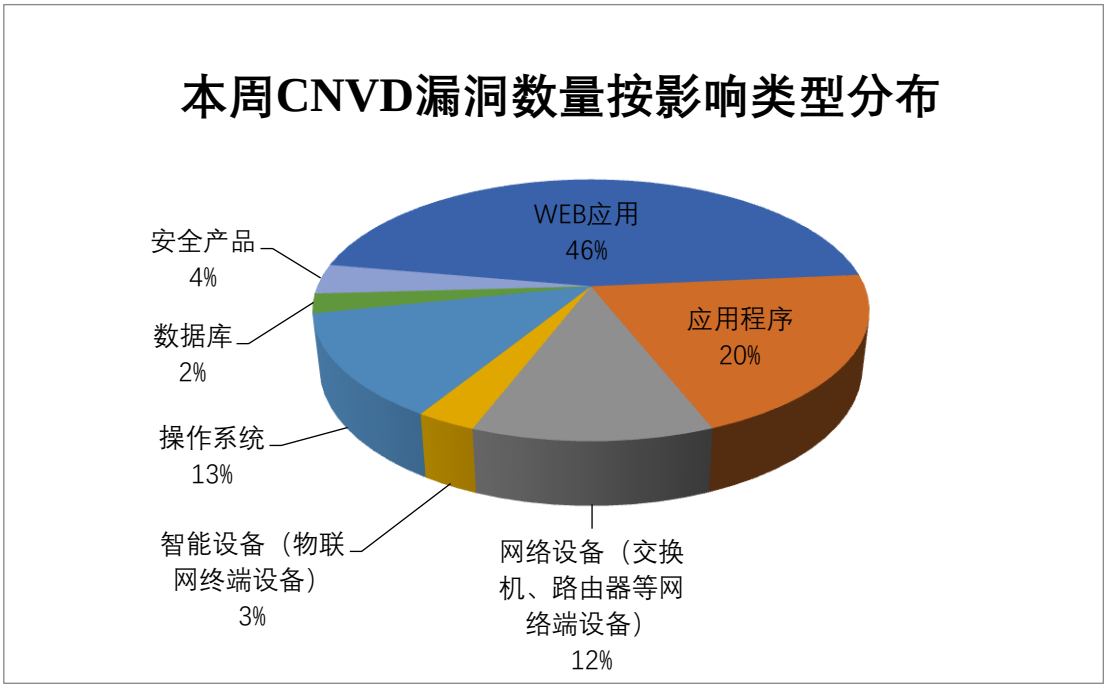

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Google、廊坊市极致网络科技有限公司、Adobe 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	Google	78	14%
2	廊坊市极致网络科技有限公司	21	4%
3	Adobe	20	4%
4	上海泛微网络科技股份有限公司	13	2%
5	WordPress	12	2%
6	MariaDB	11	2%
7	Huawei	10	2%
8	TOTOLINK	9	2%

9	Cisco	9	2%
10	其他	359	66%

本周行业漏洞收录情况

本周，CNVD 收录了 39 个电信行业漏洞，79 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，“Google Android 权限提升漏洞（CNVD-2022-43854、CNVD-2022-43855）”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/

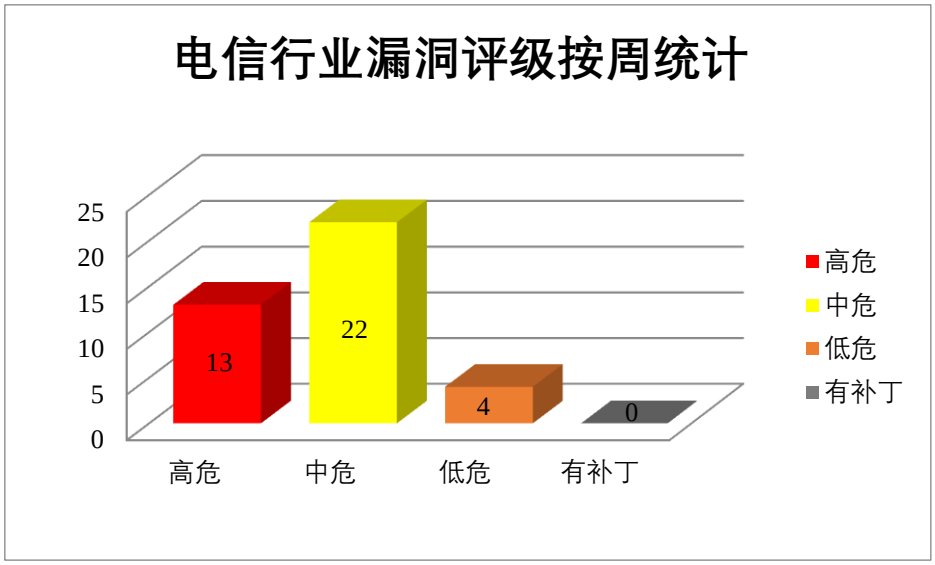

图 3 电信行业漏洞统计

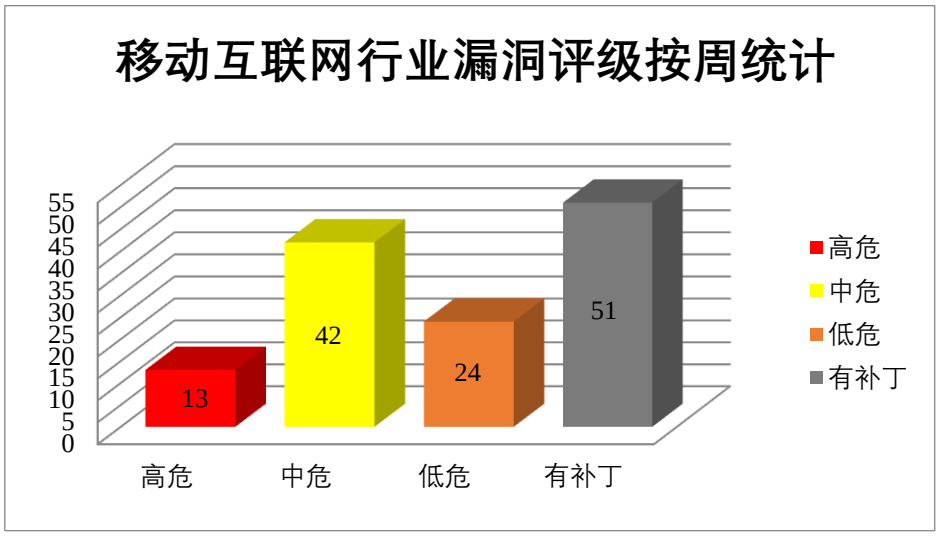

图 4 移动互联网行业漏洞统计

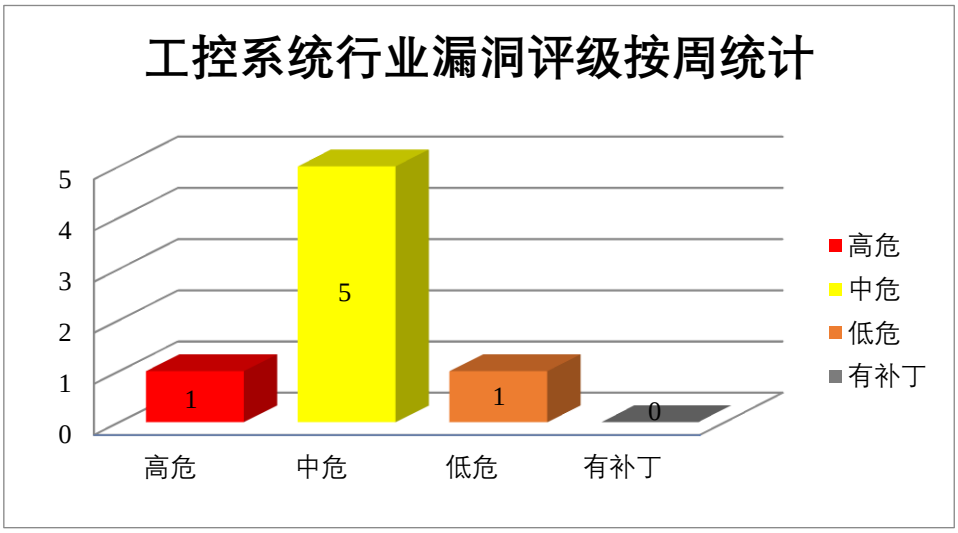

图 5 工控系统行业漏洞统计

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、 Google 产品安全漏洞

Google Android 是美国谷歌（Google）公司的一套以 Linux 为基础的开源操作系统。本周，上述产品被披露存在权限提升漏洞，攻击者可利用漏洞导致本地权限升级。

CNVD 收录的相关漏洞包括：Google Android 权限提升漏洞（CNVD-2022-43854、CNVD-2022-43857、CNVD-2022-43856、CNVD-2022-43855、CNVD-2022-44604、CNVD-2022-44607、CNVD-2022-44606、CNVD-2022-44605）。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-2022-43854

https://www.cnvd.org.cn/flaw/show/CNVD-2022-43857

https://www.cnvd.org.cn/flaw/show/CNVD-2022-43856

https://www.cnvd.org.cn/flaw/show/CNVD-2022-43855

https://www.cnvd.org.cn/flaw/show/CNVD-2022-44604

https://www.cnvd.org.cn/flaw/show/CNVD-2022-44607

https://www.cnvd.org.cn/flaw/show/CNVD-2022-44606

https://www.cnvd.org.cn/flaw/show/CNVD-2022-44605

2、 Adobe 产品安全漏洞

Adobe Acrobat 是一套 PDF 文件编辑和转换工具。Adobe Acrobat Reader 是一款 PDF 查看器。该软件用于打印，签名和注释 PDF。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：多款 Adobe 产品资源管理错误漏洞（CNVD-2022-43379、CNVD-2022-43455、CNVD-2022-43382、CNVD-2022-43380、CNVD-2022-43384、CNVD-2022-43454）、多款 Adobe 产品越界写入漏洞（CNVD-2022-43453）、多款 Adobe 产品越界读取漏洞（CNVD-2022-43383）。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-2022-43379
https://www.cnvd.org.cn/flaw/show/CNVD-2022-43383
https://www.cnvd.org.cn/flaw/show/CNVD-2022-43382
https://www.cnvd.org.cn/flaw/show/CNVD-2022-43380
https://www.cnvd.org.cn/flaw/show/CNVD-2022-43384
https://www.cnvd.org.cn/flaw/show/CNVD-2022-43454
https://www.cnvd.org.cn/flaw/show/CNVD-2022-43453
https://www.cnvd.org.cn/flaw/show/CNVD-2022-43455

3、 Huawei 产品安全漏洞

Huawei HarmonyOS 是中国华为（Huawei）公司的一个操作系统。提供一个基于微内核的全场景分布式操作系统。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞绕过 Web 身份验证并获得设备的管理访问权限，创建任意文件，进行权限提升等。

CNVD 收录的相关漏洞包括：Huawei HarmonyOS 整数溢出漏洞（CNVD-2022-44616）、Huawei HarmonyOS 授权问题漏洞（CNVD-2022-44619、CNVD-2022-44618）、Huawei HarmonyOS 目录遍历漏洞、Huawei HarmonyOS WIFI 模块权限提升漏洞、Huawei HarmonyOS 拒绝服务漏洞（CNVD-2022-44620）、Huawei HarmonyOS DFX 模块访问控制错误漏洞、Huawei HarmonyOS DFX 模块释放后重用漏洞。其中，“Huawei HarmonyOS WIFI 模块权限提升漏洞、Huawei HarmonyOS DFX 模块释放后重用漏洞”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-2022-44616
https://www.cnvd.org.cn/flaw/show/CNVD-2022-44619
https://www.cnvd.org.cn/flaw/show/CNVD-2022-44618
https://www.cnvd.org.cn/flaw/show/CNVD-2022-44617
https://www.cnvd.org.cn/flaw/show/CNVD-2022-44621
https://www.cnvd.org.cn/flaw/show/CNVD-2022-44620
https://www.cnvd.org.cn/flaw/show/CNVD-2022-44625
https://www.cnvd.org.cn/flaw/show/CNVD-2022-44624

4、 Cisco 产品安全漏洞

Cisco Firepower Threat Defense 是美国思科（Cisco）公司的一套提供下一代防火墙服务的统一软件。Cisco Firepower Management Center（FMC）是美国思科（Cisco）公司的新一代防火墙管理中心软件。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞在未经适当授权的情况下查看数据，将 XML 注入命令解析器，导致命令的意外处理和意外的命令输出，触发拒绝服务 (DoS) 条件等。

CNVD 收录的相关漏洞包括：Cisco Firepower Threat Defense 输入验证错误漏洞、Cisco Firepower Threat Defense 代码问题漏洞、Cisco Firepower Management Center 输入验证错误漏洞（CNVD-2022-43400）、Cisco Firepower Management Center 代码问题漏洞、Cisco Firepower Threat Defense 访问控制错误漏洞（CNVD-2022-43398）、Cisco Firepower Threat Defense 资源管理错误漏洞（CNVD-2022-43404）、Cisco Firepower Threat Defense 拒绝服务漏洞（CNVD-2022-43403、CNVD-2022-43402）。其中，“Cisco Firepower Threat Defense 代码问题漏洞、Cisco Firepower Management Center 代码问题漏洞、Cisco Firepower Threat Defense 资源管理错误漏洞（CNVD-2022-43404）、Cisco Firepower Threat Defense 拒绝服务漏洞（CNVD-2022-43402）”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-2022-43397
https://www.cnvd.org.cn/flaw/show/CNVD-2022-43401
https://www.cnvd.org.cn/flaw/show/CNVD-2022-43400
https://www.cnvd.org.cn/flaw/show/CNVD-2022-43399
https://www.cnvd.org.cn/flaw/show/CNVD-2022-43398
https://www.cnvd.org.cn/flaw/show/CNVD-2022-43404
https://www.cnvd.org.cn/flaw/show/CNVD-2022-43403
https://www.cnvd.org.cn/flaw/show/CNVD-2022-43402

5、Vite 目录遍历漏洞

Vite一种新型前端构建工具，能够显著提升前端开发体验。本周，Vite 被披露存在目录遍历漏洞。攻击者可利用该漏洞访问本地文件系统。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-2022-44615

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-2022-44238	GLPI 信息泄露漏洞（CNVD-2022-44238）	高	厂商已发布了漏洞修复程序，请及时关注更新：

			https://github.com/glpi-project/glpi/security/advisories/GHSA-4r49-52q9-5fgr
CNVD-2022-44244	Roothub SQL 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://github.com/miansen/Roothub/tree/v2.6
CNVD-2022-44243	Roothub SQL 注入漏洞（CNVD-2022-44243）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/miansen/Roothub/tree/v2.6
CNVD-2022-44248	WordPress stopbadbots plugin SQL 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://wpscan.com/vulnerability/a0fbb79a-e160-49df-9cf2-18ab64ea66cb
CNVD-2022-44246	WordPress Visual Form Builder plugin CSV 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://wpscan.com/vulnerability/03210390-2054-40c0-9508-39d168087878
CNVD-2022-44609	Google Android 权限提升漏洞(CNVD-2022-44609)	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/2022-03-01
CNVD-2022-44608	Google Android 权限提升漏洞（CNVD-2022-44608）	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/2022-03-01
CNVD-2022-44610	Google Android 权限提升漏洞（CNVD-2022-44610）	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/2022-03-01
CNVD-2022-43384	多款 Adobe 产品资源管理错误漏洞（CNVD-2022-43384）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：http://helpx.adobe.com/security/products/acrobat/apsb22-16.html
CNVD-2022-43399	Cisco Firepower Management Center 代码问题漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-security-bypass-JhOd29Gg

小结：本周，Google 产品被披露存在权限提升漏洞，攻击者可利用漏洞导致本地权限升级。此外，Adobe、Huawei、Cisco 等多款产品被披露存在多个漏洞，攻击者可利

用漏洞在未经适当授权的情况下查看数据，将 XML 注入命令解析器，导致命令的意外处理和意外的命令输出，触发拒绝服务 (DoS) 条件，在当前用户的上下文中执行任意代码等。另外，Vite 被披露存在目录遍历漏洞。攻击者可利用该漏洞访问本地文件系统。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、Student Grading System SQL 注入漏洞（CNVD-2022-44234）

验证描述

Student Grading System 是 Carlo Montero 个人开发者的一个学生评分系统。

Student Grading System v1.0 版本存在 SQL 注入漏洞，攻击者可利用该漏洞执行非法 SQL 命令窃取数据库敏感数据。

验证信息

POC 链接：https://github.com/k0xx11/bug_report/blob/main/vendors/oretnom23/Student-Grading-System/SQLi-1.md

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2022-44234

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. Linux 恶意软件共生体“几乎无法被检测到”

来自 BlackBerry 和 Intezer 的一组网络安全研究人员发现了一种新的 Linux 恶意软件，据两家公司称，这种恶意软件“几乎无法检测到”。

参考链接：https://www.infosecurity-magazine.com/news/linux-malware-symbiote/

2. 0Patch 为新 DogWalk Windows 零日漏洞发布非官方安全补丁

近期，0patch 研究人员针对名为 DogWalk 的 Windows 零日漏洞发布了一个非官方的安全补丁。

参考链接：https://securityaffairs.co/wordpress/132070/hacking/unofficial-security-patch-dogwalk.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