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 20 日-2022 年 06 月 26 日 **2022 年第 25 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 383 个，其中高危漏洞 149 个、中危漏洞 202 个、低危漏洞 32 个。漏洞平均分值为 6.03。本周收录的漏洞中，涉及 0day 漏洞 290 个（占 76%），其中互联网上出现“WordPress WP Contacts Manager SQL 注入漏洞、Jfinal CMS 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 8658 个，与上周（9231 个）环比减少 6%。

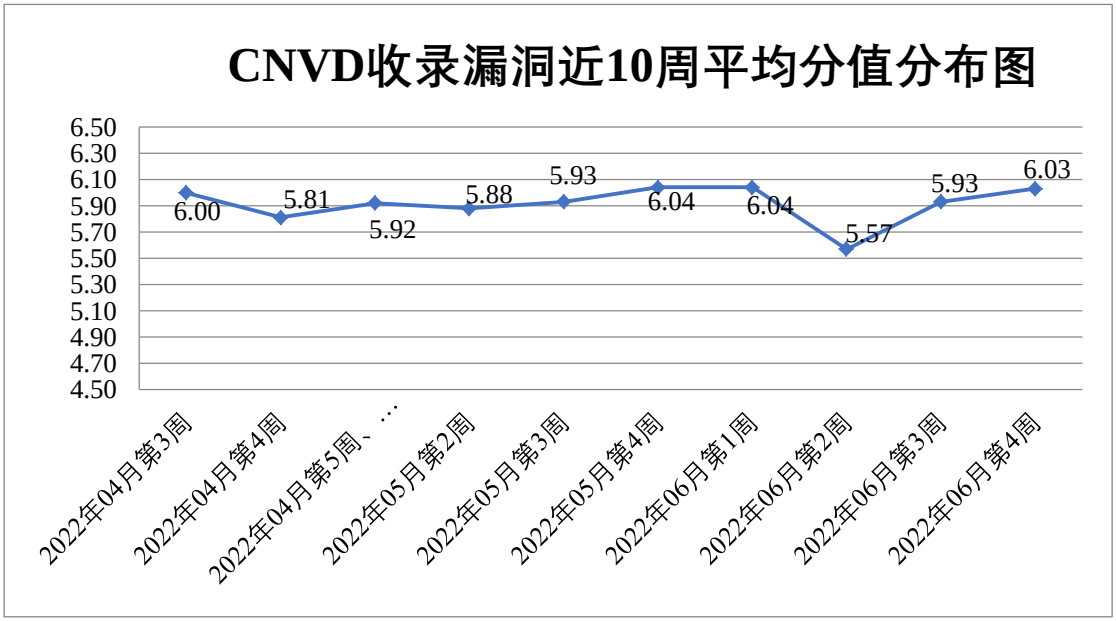

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 22 起，向基础电信企业通报漏洞事件 32 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 697 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 125 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 112 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：

重庆梅安森科技股份有限公司、友讯电子设备（上海）有限公司、兄弟（中国）商业有限公司、夏普商贸（中国）有限公司、武汉金同方科技有限公司、卫宁健康科技集团股份有限公司、微软（中国）有限公司、苏州祥云平台信息技术有限公司、苏州思迪信息技术有限公司、四川千行你我科技股份有限公司、深圳智沃科技有限公司、深圳维盟科技股份有限公司、深圳市图美电子技术有限公司、深圳市锐明技术股份有限公司、深圳市吉祥腾达科技有限公司、上海卓卓网络科技有限公司、上海茸易科技有限公司、瑞斯康达科技发展股份有限公司、普联技术有限公司、明腾网络股份有限公司、联想图像（北京）科技有限公司、廊坊市极致网络科技有限公司、惠普贸易（上海）有限公司、华硕电脑（上海）有限公司、湖南省思派电子科技有限公司、湖南快乐阳光互动娱乐传媒有限公司、湖南建研信息技术股份有限公司、洪湖尔创网联信息技术有限公司、恒锋信息科技股份有限公司、杭州雄伟科技开发股份有限公司、杭州恒生数字设备科技有限公司、广州红帆科技有限公司、广东顶固集创家居股份有限公司、北京卓易讯畅科技有限公司、北京致远互联软件股份有限公司、北京易勤信息技术有限公司、北京亿赛通科技发展有限责任公司、北京星网锐捷网络技术有限公司、北京信安世纪科技股份有限公司、北京网康科技有限公司、北京万户网络技术有限公司、北京通达志成科技有限公司、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、北京良精志诚科技有限责任公司、北京九思协同软件有限公司、北京宝兰德软件股份有限公司、北京百卓网络技术有限公司、网展科技、宝利通公司、易迅软件工作室、The Apache Software Foundation、Texas Instruments、ST Engineering iDirect, Inc. dba iDirect、SEMCMS、JFinalOA 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，新华三技术有限公司、深信服科技股份有限公司、北京神州绿盟科技有限公司、北京数字观星科技有限公司、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。重庆都会信息科技有限公司、上海纽盾科技股份有限公司、杭州默安科技有限公司、河南东方云盾信息技术有限公司、北京安盟信息技术股份有限公司、河南灵创电子科技有限公司、北京天地和兴科技有限公司、河南信安世纪科技有限公司、北京升鑫网络科技有限公司、厦门捷诺通信息技术股份有限公司、新疆海狼科技有限公司、北京云科安信科技有限公司（Seraph 安全实验室）、浙江木链物联网科技有限公司、中国电信股份有限公司甘肃分公司、贵州泰若数字科技有限公司、

江苏国泰新点软件有限公司、广州百蕴启辰科技有限公司、思而听网络科技有限公司及其他个人白帽子向 CNVD 提交了 8658 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）、上海交大和奇安信网神（补天平台）向 CNVD 共享的白帽子报送的 6964 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）	3424	3424
奇安信网神（补天平台）	3325	3325
新华三技术有限公司	437	0
深信服科技股份有限公司	390	0
北京神州绿盟科技有限公司	337	0
北京数字观星科技有限公司	253	0
上海交大	215	215
安天科技集团股份有限公司	206	0
天津市国瑞数码安全系统股份有限公司	118	0
恒安嘉新（北京）科技股份公司	103	0
北京天融信网络安全技术有限公司	93	0
北京启明星辰信息安全技术有限公司	68	0
京东科技信息技术有限公司	54	32
中国电信集团系统集成有限责任公司	25	0
杭州安恒信息技术股份有限公司	22	22
远江盛邦（北京）网络安全科技股份有限	22	22

公司		
西安四叶草信息技术有限公司	15	15
北京知道创宇信息技术有限公司	8	0
卫士通信息产业股份有限公司	6	6
内蒙古云科数据服务股份有限公司	5	5
南京联成科技发展股份有限公司	4	4
北京信联科汇科技有限公司	1	1
北京华顺信安科技有限公司	247	0
墨菲未来科技(北京)有限公司	173	0
重庆都会信息科技有限公司	100	100
上海纽盾科技股份有限公司	49	49
杭州默安科技有限公司	39	39
河南东方云盾信息技术有限公司	17	17
北京安盟信息技术股份有限公司	15	15
河南灵创电子科技有限公司	10	10
北京天地和兴科技有限公司	9	9
河南信安世纪科技有限公司	5	5
北京升鑫网络科技有限公司	5	5

厦门捷诺通信息技术股份有限公司	2	2
新疆海狼科技有限公司	2	2
北京云科安信科技有限公司（Seraph 安全实验室）	2	2
亚信科技（成都）有限公司	1	0
浙江木链物联网科技有限公司	1	1
中国电信股份有限公司甘肃分公司	1	1
贵州泰若数字科技有限公司	1	1
江苏国泰新点软件有限公司	1	1
西门子（中国）有限公司	1	0
广州百蕴启辰科技有限公司	1	1
思而听网络科技有限公司	1	1
CNCERT 内蒙古分中心	7	7
CNCERT 贵州分中心	2	2
个人	1317	1317
报送总计	11140	8658

本周漏洞按类型和厂商统计

本周，CNVD 收录了 383 个漏洞。WEB 应用 206 个，应用程序 80 个，网络设备（交换机、路由器等网络端设备）56 个，操作系统 20，智能设备（物联网终端设备）11 个个，安全产品 8 个，数据库 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	206
应用程序	80
网络设备（交换机、路由器等网络端设备）	56
操作系统	20
智能设备（物联网终端设备）	11
安全产品	8
数据库	2

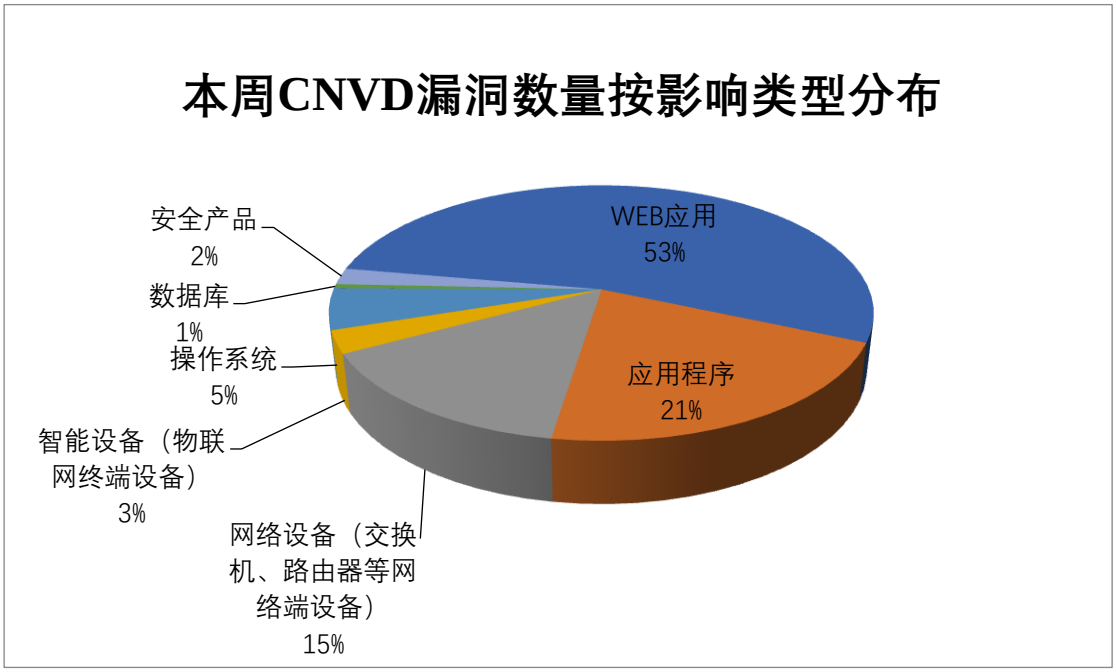

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Adobe、WordPress、Google 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	28	7%
2	WordPress	27	7%
3	Google	16	4%
4	Cisco	13	3%
5	IBM	13	3%
6	Tenda	7	2%
7	Billing Management System	7	2%
8	D-Link	7	2%
9	北京星网锐捷网络技术有	6	2%

	限公司		
10	其他	259	68%

本周行业漏洞收录情况

本周，CNVD 收录了 43 个电信行业漏洞，22 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，“Xiaomi Router AX3600 命令注入漏洞、Siemens SIMATIC WinCC OA 客户端身份验证漏洞”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/

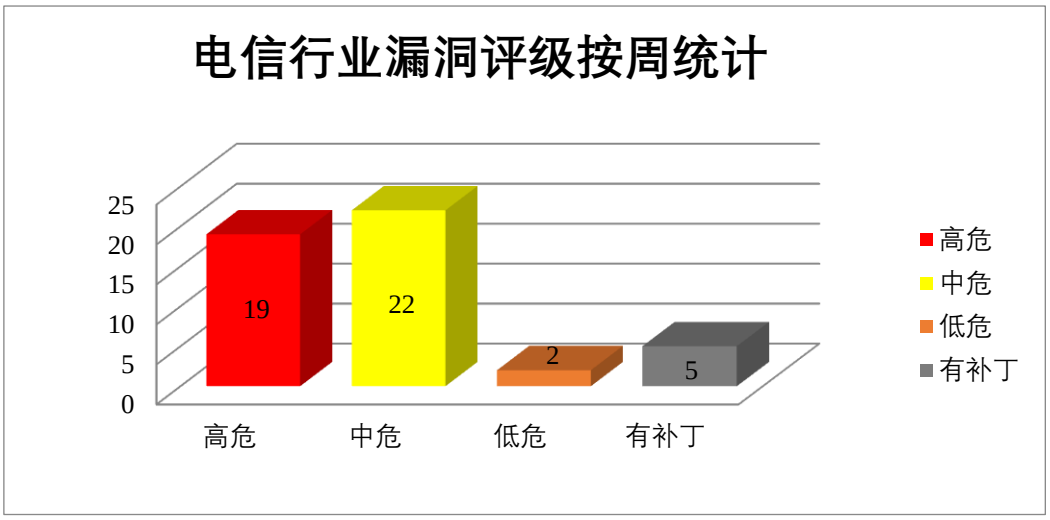

图 3 电信行业漏洞统计

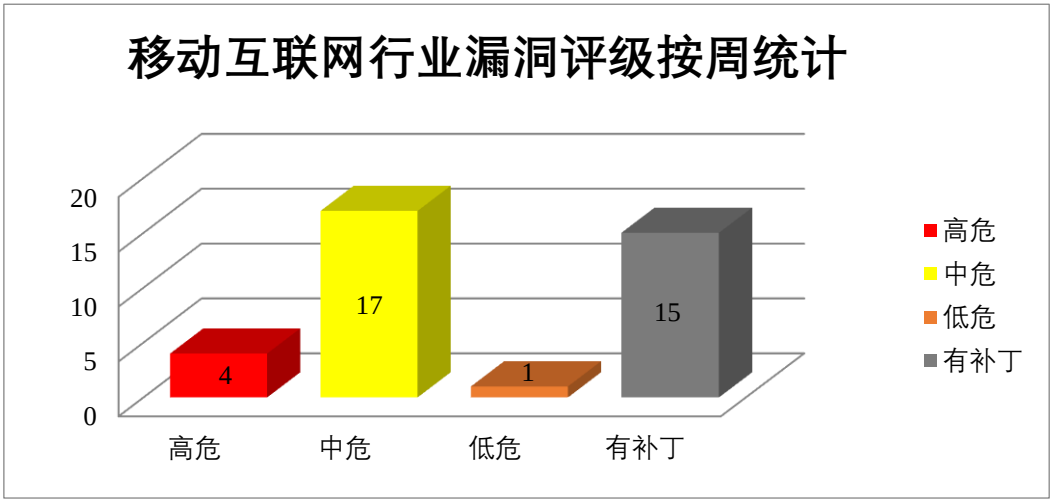

图 4 移动互联网行业漏洞统计

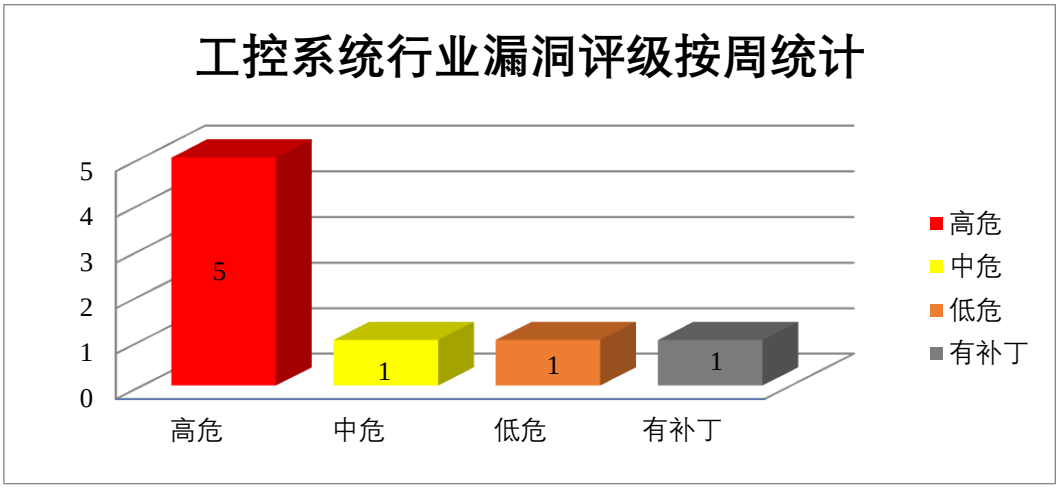

图 5 工控系统行业漏洞统计

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 Acrobat 是一套 PDF 文件编辑和转换工具。Adobe Acrobat Reader 是一款 PDF 查看器。Adobe Reader 是一套 PDF 文档阅读软件。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-2022-46965、CNVD-2022-46966、CNVD-2022-46971、CNVD-2022-46970、CNVD-2022-46972、CNVD-2022-46977、CNVD-2022-46976、CNVD-2022-46975）。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-2022-46965

https://www.cnvd.org.cn/flaw/show/CNVD-2022-46966

https://www.cnvd.org.cn/flaw/show/CNVD-2022-46971

https://www.cnvd.org.cn/flaw/show/CNVD-2022-46970

https://www.cnvd.org.cn/flaw/show/CNVD-2022-46972

https://www.cnvd.org.cn/flaw/show/CNVD-2022-46977

https://www.cnvd.org.cn/flaw/show/CNVD-2022-46976

https://www.cnvd.org.cn/flaw/show/CNVD-2022-46975

2、 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多个漏洞，攻击者可利用漏洞导致本地权限升级，文件选择器中的远程持续拒绝服务等。

CNVD 收录的相关漏洞包括：Google Android 缓冲区溢出漏洞（CNVD-2022-46292、CNVD-2022-46298、CNVD-2022-46301、CNVD-2022-46294、CNVD-2022-46293）、Google Android 拒绝服务漏洞（CNVD-2022-46296、CNVD-2022-46290）、Google Android 越界写入漏洞（CNVD-2022-46299）。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-2022-46292
https://www.cnvd.org.cn/flaw/show/CNVD-2022-46290
https://www.cnvd.org.cn/flaw/show/CNVD-2022-46294
https://www.cnvd.org.cn/flaw/show/CNVD-2022-46293
https://www.cnvd.org.cn/flaw/show/CNVD-2022-46296
https://www.cnvd.org.cn/flaw/show/CNVD-2022-46299
https://www.cnvd.org.cn/flaw/show/CNVD-2022-46298
https://www.cnvd.org.cn/flaw/show/CNVD-2022-46301

3、IBM 产品安全漏洞

IBM Planning Analytics 是美国 IBM 公司的一套业务规划分析解决方案。该方案支持自动化执行业务规划、预算和分析等流程。IBM Security Identity Manager（ISIM）是一套身份管理和治理解决方案。IBM UrbanCode Deploy（UCD）是一套应用自动化部署工具。IBM Security Guardium 是一套提供数据保护功能的平台。IBM System Storage DS8000 Hardware Management Console 是一个 IBM 存储介质平台 DS8000 的硬件管理控制台。IBM Sterling B2B Integrator 是一套集成了重要的 B2B 流程、交易和关系的软件。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。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，上传任意可执行文件，导致代码执行，造成拒绝服务等。

CNVD 收录的相关漏洞包括：IBM Planning Analytics 任意文件上传漏洞、IBM Security Identity Manager 缓冲区溢出漏洞（CNVD-2022-46305）、IBM UrbanCode Deploy 权限提升漏洞（CNVD-2022-46304）、IBM Security Guardium 信息泄露漏洞（CNVD-2022-46310）、IBM Planning Analytics 服务端请求伪造漏洞、IBM System Storage DS8000 Hardware Management Console 信息泄露漏洞、IBM Sterling B2B Integrator 跨站请求伪造漏洞(CNVD-2022-46459)、IBM Aspera High-Speed Transfer 信息泄露漏洞。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-2022-46306
https://www.cnvd.org.cn/flaw/show/CNVD-2022-46305
https://www.cnvd.org.cn/flaw/show/CNVD-2022-46304
https://www.cnvd.org.cn/flaw/show/CNVD-2022-46310

https://www.cnvd.org.cn/flaw/show/CNVD-2022-46457

https://www.cnvd.org.cn/flaw/show/CNVD-2022-46460

https://www.cnvd.org.cn/flaw/show/CNVD-2022-46459

https://www.cnvd.org.cn/flaw/show/CNVD-2022-46458

4、Cisco 产品安全漏洞

Cisco Embedded Wireless Controller 是美国思科（Cisco）公司的一个无线接入器。Cisco SD-WAN vManage Software 是一款用于 SD-WAN（软件定义广域网络）解决方案的管理软件。Cisco Virtualized Infrastructure Manager 是一个完全自动化的云生命周期管理系统。Cisco Wireless LAN Controller（WLC）是一款无线局域网控制器产品。Cisco SD-WAN vManage Software 是一款用于 SD-WAN（软件定义广域网络）解决方案的管理软件。Cisco Catalyst Digital Building Series Switches 是一系列数字楼宇交换机。Cisco Iox 是一个结合了 Cisco IOS 和 Linux OS 用于安全网络连接以及开发 IOT 应用的安全开发环境。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞导致设备重新加载，以受影响用户的权限级别执行任意操作，访问机密信息并提升受影响设备的权限等。

CNVD 收录的相关漏洞包括：Cisco Embedded Wireless Controller 拒绝服务漏洞、Cisco SD-WAN vManage Software 跨站请求伪造漏洞、Cisco Virtualized Infrastructure Manager 访问控制错误漏洞、Cisco Wireless LAN Controller 身份验证绕过漏洞、Cisco SD-WAN vManage Software 信息泄露漏洞（CNVD-2022-46480）、Cisco Catalyst Digital Building Series Switches and Cisco Catalyst Micro Switches 拒绝服务漏洞、Cisco Iox 路径遍历漏洞、Cisco Iox 拒绝服务漏洞。其中，“Cisco Embedded Wireless Controller 拒绝服务漏洞、Cisco Wireless LAN Controller 身份验证绕过漏洞”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-2022-46478

https://www.cnvd.org.cn/flaw/show/CNVD-2022-46477

https://www.cnvd.org.cn/flaw/show/CNVD-2022-46475

https://www.cnvd.org.cn/flaw/show/CNVD-2022-46481

https://www.cnvd.org.cn/flaw/show/CNVD-2022-46480

https://www.cnvd.org.cn/flaw/show/CNVD-2022-46479

https://www.cnvd.org.cn/flaw/show/CNVD-2022-46961

https://www.cnvd.org.cn/flaw/show/CNVD-2022-46962

5、WordPress Domain Replace plugin 跨站脚本漏洞

WordPress 和 WordPress plugin 都是 WordPress 基金会的产品。WordPress 是一套使用 PHP 语言开发的博客平台。该平台支持在 PHP 和 MySQL 的服务器上架设个人博客

网站。WordPress plugin 是一个应用插件。本周，WordPress Domain Replace plugin 被披露存在跨站脚本漏洞。攻击者可利用该漏洞导致反射跨站点脚本攻击。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-2022-46774

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-2022-46464	WordPress SpeakOut! Email Petitions 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/b030296d-688e-44a4-a48a-140375f2c5f4
CNVD-2022-46968	多款 Adobe 产品越界写入漏洞（CNVD-2022-46968）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://helpx.adobe.com/security/products/acrobat/apsb22-16.html
CNVD-2022-46967	多款 Adobe 产品越界写入漏洞（CNVD-2022-46967）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://helpx.adobe.com/security/products/acrobat/apsb22-16.html
CNVD-2022-46969	多款 Adobe 产品堆栈缓冲区溢出漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://helpx.adobe.com/security/products/acrobat/apsb22-16.html
CNVD-2022-46974	多款 Adobe 产品越界写入漏洞（CNVD-2022-46974）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://helpx.adobe.com/security/products/acrobat/apsb22-16.html
CNVD-2022-47336	Xiaomi Router AX3600 命令注入漏洞（CNVD-2022-47336）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://trust.mi.com/zh-CN/misrc/bulletins/advisory?cveId=37
CNVD-2022-47422	WordPress Nirweb support 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/1a8f9c7b-a422-4f45-a516-c3c14eb05161
CNVD-2022-46963	Siemens SIMATIC WinCC OA 客户端身份验证漏洞	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://cert-portal.siemens.com/productcert/html/ssa-111512.html
CNVD-2022	多款 Adobe 产品资源管理错	高	目前厂商已发布升级补丁以修复漏

-46966	误漏洞（CNVD-2022-46966）		洞，补丁获取链接：https://helpx.adobe.com/security/products/acrobat/apsb22-16.html
CNVD-2022-46971	多款 Adobe 产品资源管理错误漏洞（CNVD-2022-46971）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://helpx.adobe.com/security/products/acrobat/apsb22-16.html

小结：本周，Adobe 产品被披露存在多个漏洞，攻击者可利用漏洞在当前用户的上下文中执行任意代码。此外，Google、IBM、Cisco 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，上传任意可执行文件，导致代码执行，拒绝服务，本地权限升级等。另外，WordPress Domain Replace plugin 被披露存在跨站脚本漏洞。攻击者可利用漏洞导致反射跨站点脚本攻击。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、Jfinal CMS SQL 注入漏洞

验证描述

Jfinal CMS 是一个 java 开发的功能强大的信息咨询网站，采用了简洁强大的 JFinal 作为 web 框架，模板引擎用的是 beetl，数据库用 mysql，前端 bootstrap 框架。

Jfinal CMS 5.1 版本存在 SQL 注入漏洞，该漏洞源于/admin/folder 路径直接拼接了来自 getOrderby 函数，攻击者可利用该漏洞进行 SQL 注入攻击。

验证信息

POC 链接：https://github.com/jflyfox/jfinal_cms/issues/35

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2022-47415

信息提供者

恒安嘉新（北京）科技股份公司

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. QNAP 发出警告，PHP 漏洞可导致远程代码执行

中国台湾著名厂商 QNAP 正在解决一个 PHP 漏洞，该漏洞追踪为 CVE-2019-11043，可被用来实现远程代码执行。

参考链接：https://securityaffairs.co/wordpress/132531/hacking/qnap-critical-php-vulnerabil

ity.html

2. SmartTub 功能存在安全漏洞，智能按摩浴缸泄露用户数据

安全研究人员发现世界知名按摩浴缸品牌生产的热水浴缸中使用的应用程序 Smart Tub 功能存在安全漏洞，允许攻击者查看和滥用热水浴缸用户的个人数据。

参考链接：https://www.hackread.com/smart-jacuzzi-app-flaw-exploited-extract-user-data/

关于 CNVD

国家信息安全漏洞共享平台（China National Vulnerability Database，简称 CNVD）是 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信息安全漏洞信息共享知识库，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，是我国网络安全应急体系的核心协调机构。

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