国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2021 年 05 月 17 日-2021 年 05 月 23 日　　2021 年第 20 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 581 个，其中高危漏洞 120 个、中危漏洞 374 个、低危漏洞 87 个。漏洞平均分值为 5.40。本周收录的漏洞中，涉及 0day 漏洞 323 个（占 56%），其中互联网上出现“OpenEMR 操作系统命令注入漏洞、PHPGurukul Online Book Store 任意文件上传漏洞”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 3079 个，与上周（2544 个）环比增加 21%。

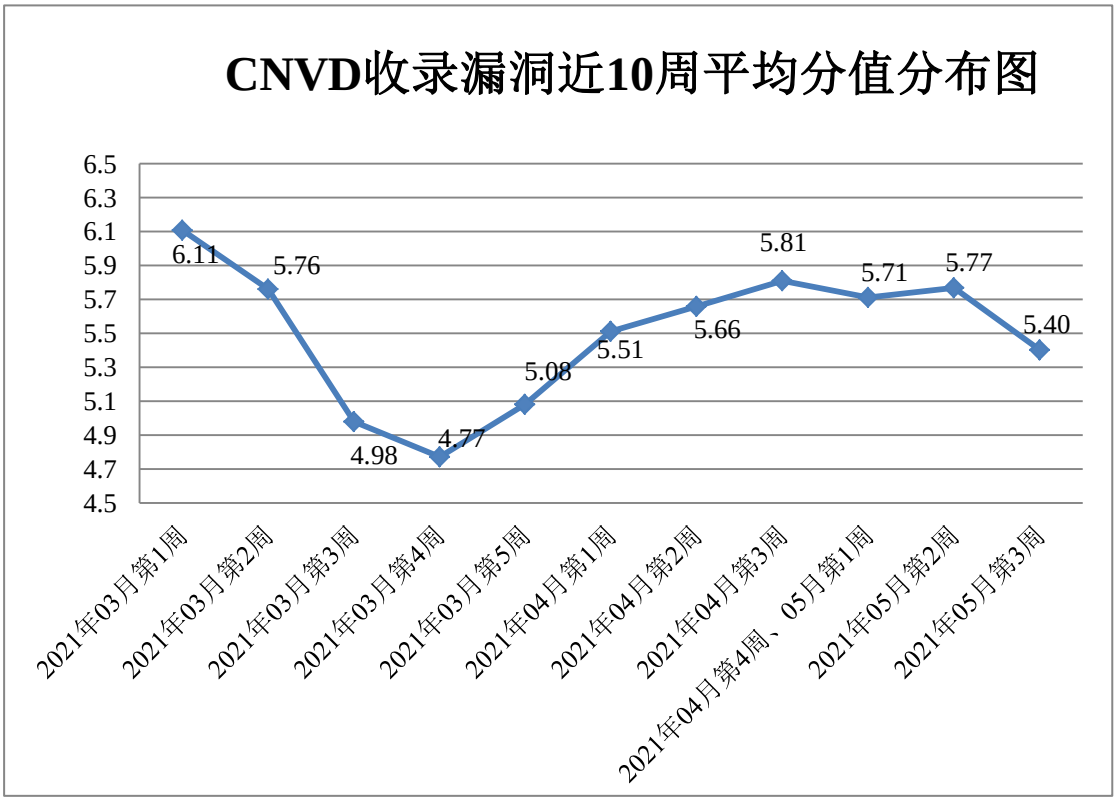

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 28 起，向基础电信企业通报漏洞事件 19 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 434 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 77 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 60 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：

作业帮教育科技（北京）有限公司、淄博闪灵网络科技有限公司、诸城三剑网络传媒有限公司、长沙友点软件科技有限公司、友讯电子设备（上海）有限公司、用友网络科技股份有限公司、武汉天地伟业科技有限公司、网易有道信息技术（北京）有限公司、统信软件技术有限公司、天信仪表集团有限公司、天地伟业技术有限公司、台达电子企业管理（上海）有限公司、宿迁鑫潮信息技术有限公司、苏州祥云平台信息技术有限公司、苏州汉明科技有限公司、搜狗科技发展有限公司、四平市九州易通科技有限公司、四创科技有限公司、石家庄市轨道交通有限责任公司、深圳维盟科技股份有限公司、深圳市英威腾电气股份有限公司、深圳市迅捷通信技术有限公司、深圳市腾狐物联科技有限公司、深圳市美科星通信技术有限公司、深圳市领空技术有限公司、深圳市锟铻科技有限公司、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、深圳市惠尔顿信息技术有限公司、深圳市华磊信息科技有限公司、深圳市阿迪通科技有限公司、深圳前海天智信息技术有限公司、上海装盟信息科技有限公司、上海智休信息科技有限公司、上海云轴信息科技有限公司、上海创旗天下科技股份有限公司、上海博达数据通信有限公司、上海宝信软件股份有限公司、上海艾泰科技有限公司、山东思达特测控设备有限公司、山东比特智能科技股份有限公司、厦门狮子鱼网络科技有限公司、厦门三五互联科技股份有限公司、润申信息科技（上海）有限公司、锐捷网络股份有限公司、泉州微笑自行车有限公司、全讯汇聚网络科技（北京）有限公司、普联技术有限公司、南宁比优网络科技有限公司、迈普通信技术股份有限公司、昆明鼎华信息科技有限公司、科大讯飞股份有限公司、康普科技（苏州）有限公司、聚乐网络科技（深圳）有限公司、京源中科科技股份有限公司、江苏安科瑞电器制造有限公司、杭州图特信息科技有限公司、杭州三汇信息工程有限公司、杭州海康威视数字技术股份有限公司、杭州鼎易信息科技有限公司、汉王科技股份有限公司、海湾安全技术有限公司、国电南瑞科技股份有限公司、桂林佳朋信息科技有限公司、广州网易计算机系统有限公司、广州图创计算机软件开发有限公司、广东南方数码科技有限公司、光洋电子（无锡）有限公司、谷歌公司、甘肃睿阳科技有限公司、德化县艺创陶瓷有限公司、成都星锐蓝海网络科技有限公司、成都市智蜂网科技有限责任公司、成都飞鱼星科技股份有限公司、北京中控科技发

展有限公司、北京中科联诚软件股份有限公司、北京中创视讯科技有限公司、北京印象笔记科技有限公司、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、北京文网亿联科技有限公司、北京网康科技有限公司、北京通达信科科技有限公司、北京润尼尔网络科技有限公司、北京恰维网络科技有限公司、北京金山办公软件股份有限公司、北京百卓网络技术有限公司、百度在线网络技术（北京）有限公司、八维通科技有限公司、安美世纪（北京）科技有限公司、ACTi（中国）公司、杰科网络设计工作室、齐鲁书画网、鱼跃 CMS、ZZCMS、Zyxel、YCCMS、Victor CMS、Teledyne FLIR、SEMCMS、Online Ordering System、NETGEAR、iCMS、cyberbiz、cszcms、CourseSEL 和 CatfishCMS。

本周，CNVD 发布了《CNVD 工控漏洞子库（ICS-CNVD）正式上线》、《Microsoft 发布 2021 年 5 月安全更新》。详情参见 CNVD 网站公告内容。

https://www.cnvd.org.cn/webinfo/show/6431

https://www.cnvd.org.cn/webinfo/show/6436

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、哈尔滨安天科技集团股份有限公司、北京神州绿盟科技有限公司、北京启明星辰信息安全技术有限公司、华为技术有限公司等单位报送公开收集的漏洞数量较多。南京众智维信息科技有限公司、北京信联科汇科技有限公司、北京山石网科信息技术有限公司、安徽长泰信息安全服务有限公司、杭州海康威视数字技术股份有限公司、河南灵创电子科技有限公司、北京华云安信息技术有限公司、北京天地和兴科技有限公司、杭州木链物联网科技有限公司、小安（北京）科技有限公司、福建省海峡信息技术有限公司、山东云天安全技术有限公司、武汉明嘉信信息安全检测评估有限公司、北京顶象技术有限公司、江西省掌控者信息安全技术有限公司、河南信安世纪科技有限公司、北京墨云科技有限公司、北京安帝科技有限公司、浙江御安信息技术有限公司、北京聚信得仁科技有限公司、杭州美创科技有限公司、京东云安全、广西塔易信息技术有限公司、广州安亿信软件科技有限公司、黑龙江安衡讯信息安全测评技术服务有限公司、武汉绿色网络信息服务有限责任公司、北京机沃科技有限公司及其他个人白帽子向 CNVD 提交了 3079 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）和上海交大向 CNVD 共享的白帽子报送的 1680 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	原创漏洞数量
奇安信网神（补天平台）	954	954

北京天融信网络安全技术有限公司	439	4
斗象科技（漏洞盒子）	438	438
上海交大	288	288
哈尔滨安天科技集团股份有限公司	262	0
北京神州绿盟科技有限公司	235	2
北京启明星辰信息安全技术有限公司	178	8
华为技术有限公司	149	0
深信服科技股份有限公司	125	0
新华三技术有限公司	65	0
天津市国瑞数码安全系统股份有限公司（国瑞数码零点实验室）	59	0
恒安嘉新（北京）科技股份公司	57	0
卫士通信息产业股份有限公司	55	0
中国电信集团系统集成有限责任公司	54	54
北京数字观星科技有限公司	51	0
北京奇虎科技有限公司	25	3
南京联成科技发展股份有限公司	3	3
北京知道创宇信息技术股份有限公司	1	0
南京众智维信息科技有限公司	139	139
北京信联科汇科技有限公司	69	69
北京山石网科信息技术有限公司	45	45
安徽长泰信息安全服务有限公司	41	41
杭州海康威视数字技术股份有限公司	41	41

河南灵创电子科技有限公司	27	27
北京华云安信息技术有限公司	26	26
北京天地和兴科技有限公司	23	23
杭州木链物联网科技有限公司	21	21
杭州迪普科技股份有限公司	19	0
中国电信股份有限公司网络安全产品运营中心	15	0
小安（北京）科技有限公司	14	14
福建省海峡信息技术有限公司	11	11
山东云天安全技术有限公司	9	9
武汉明嘉信信息安全检测评估有限公司	9	9
北京顶象技术有限公司	8	8
江西省掌控者信息安全技术有限公司	7	7
河南信安世纪科技有限公司	7	7
北京墨云科技有限公司	6	6
北京安帝科技有限公司	5	5
浙江御安信息技术有限公司	5	5
北京聚信得仁科技有限公司	2	2
杭州美创科技有限公司	2	2
西门子（中国）有限公司	2	0
京东云安全	1	1
广西塔易信息技术有限公司	1	1

广州安亿信软件科技有限公司	1	1
黑龙江安衡讯信息安全测评技术服务有限公司	1	1
武汉绿色网络信息服务有限责任公司	1	1
北京机沃科技有限公司	1	1
CNCERT 宁夏分中心	11	11
CNCERT 青海分中心	10	10
CNCERT 山西分中心	1	1
个人	780	780
报送总计	4779	3079

本周漏洞按类型和厂商统计

本周，CNVD 收录了 581 个漏洞。应用程序 243 个，WEB 应用 197 个，网络设备（交换机、路由器等网络端设备）113 个，智能设备（物联网终端设备）13 个，安全产品 8 个，操作系统 6 个，数据库 1 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
应用程序	243
WEB 应用	197
网络设备（交换机、路由器等网络端设备）	113
智能设备（物联网终端设备）	13
安全产品	8
操作系统	6
数据库	1

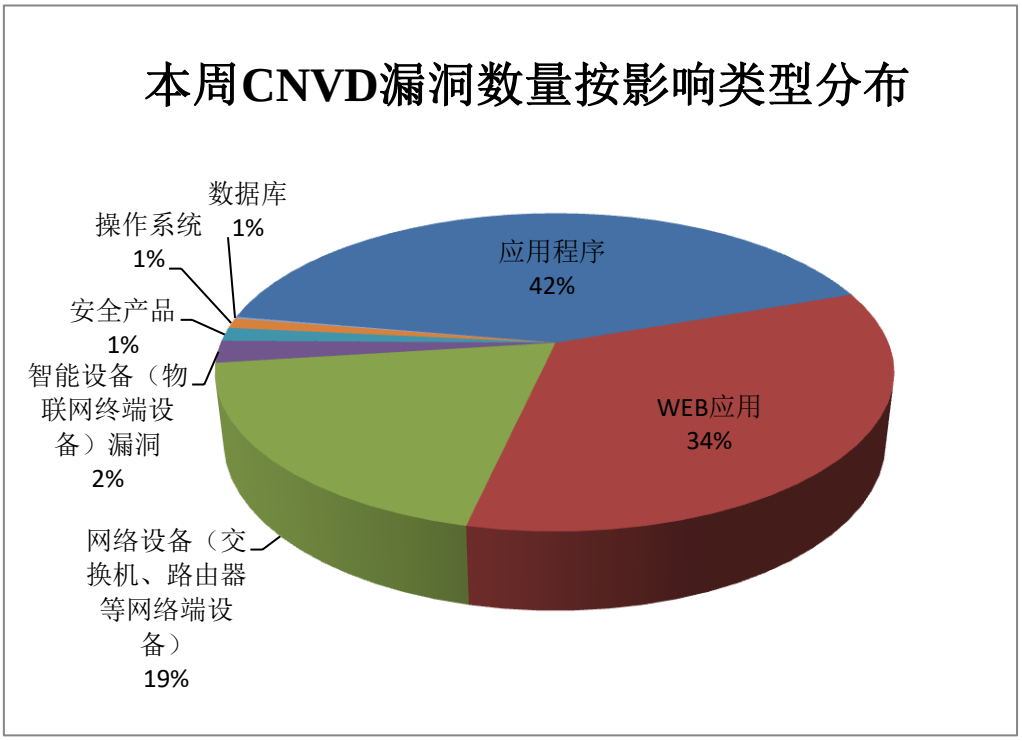

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Google、WordPress、ASUS 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	50	9%
2	WordPress	48	8%
3	ASUS	17	3%
4	JetBrains	13	2%
5	D-Link	13	2%
6	Cisco	12	2%
7	浙江大华技术股份有限公司	12	2%
8	Foxit	12	2%
9	廊坊市极致网络科技有限公司	11	2%
10	其他	393	68%

本周行业漏洞收录情况

本周，CNVD 收录了 61 个电信行业漏洞，18 个移动互联网行业漏洞，15 个工控行业漏洞（如下图所示）。其中，“TP-Link TL-WR802N（US）和 Archer_C50v5_US 缓冲区溢出漏洞、NVMS ABB Ability Ellipse APM 跨站脚本漏洞、Google Android pb_write 权限提升漏洞 、Omron CX-One 缓冲区溢出漏洞（CNVD-2021-36103）、Cisco Unif

ied Communications Manager 和 Cisco Unity Connection 代码注入漏洞”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/

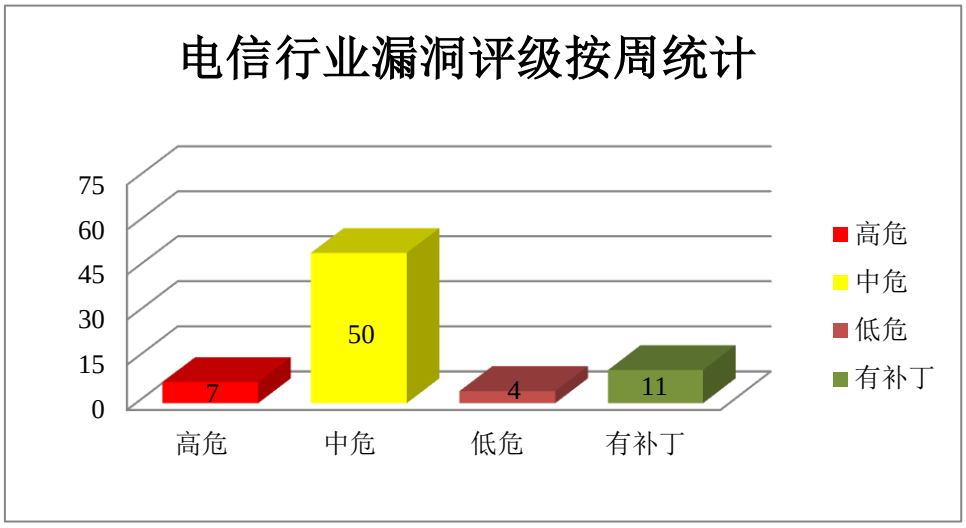

图 3 电信行业漏洞统计

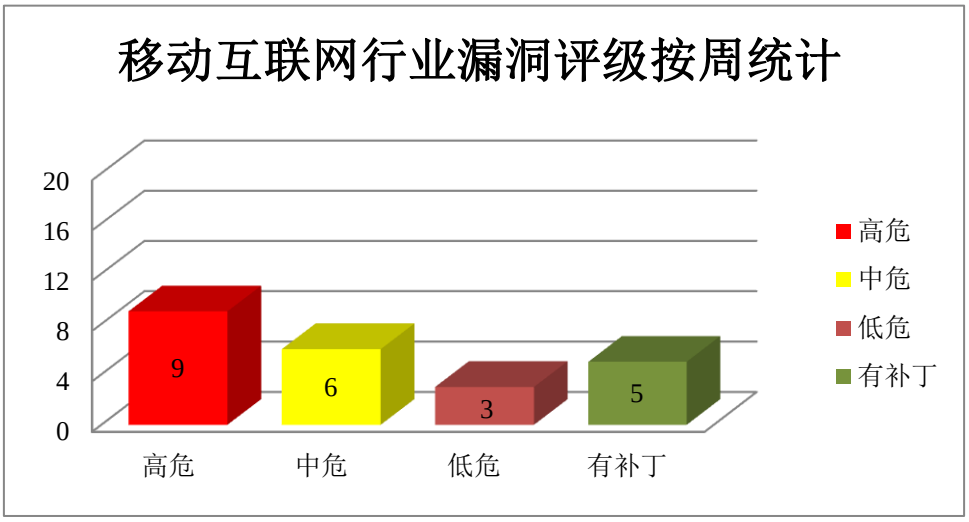

图 4 移动互联网行业漏洞统计

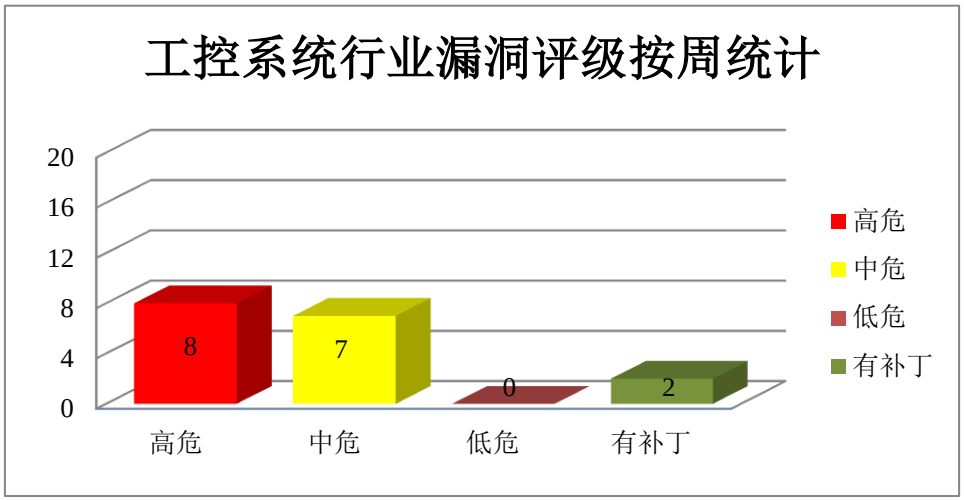

图 5 工控系统行业漏洞统计

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、Google 产品安全漏洞

Google Chrome 是美国谷歌（Google）公司的一款 Web 浏览器。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的 HTML 页面执行域欺骗，绕过安全限制，执行任意代码或造成拒绝服务等。

CNVD 收录的相关漏洞包括：Google Chrome Dev Tools 代码执行漏洞、Google Chrome ANGLE 堆缓冲区溢出漏洞、Google Chrome UI 下载安全绕过漏洞、Google Chrome IndexedDB 代码执行漏洞、Google Chrome Network 安全绕过漏洞、Google Chrome 安全绕过漏洞（CNVD-2021-35168）、Google Chrome Blink 代码执行漏洞、Google Chrome navigation 安全绕过漏洞。其中，“Google Chrome ANGLE 堆缓冲区溢出漏洞、Google Chrome UI 下载安全绕过漏洞”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-2021-35167
https://www.cnvd.org.cn/flaw/show/CNVD-2021-35166
https://www.cnvd.org.cn/flaw/show/CNVD-2021-35164
https://www.cnvd.org.cn/flaw/show/CNVD-2021-35171
https://www.cnvd.org.cn/flaw/show/CNVD-2021-35169
https://www.cnvd.org.cn/flaw/show/CNVD-2021-35168
https://www.cnvd.org.cn/flaw/show/CNVD-2021-35173
https://www.cnvd.org.cn/flaw/show/CNVD-2021-35172

2、Foxit 产品安全漏洞

Foxit Reader 是中国福昕（Foxit）公司的一款 PDF 文档阅读器。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，在当前进程的上下文中执行代码。

CNVD 收录的相关漏洞包括：Foxit Reader U3D 文件解析越界读取信息泄露漏洞（CNVD-2021-36471、CNVD-2021-36468、CNVD-2021-36473、CNVD-2021-36472）、Foxit Reader U3D 文件解析越界写入远程代码执行漏洞、Foxit Reader U3D 文件解析越界读取远程代码执行漏洞、Foxit Reader app.media 远程代码执行漏洞、Foxit Reader U3D 文件解析双重释放远程代码执行漏洞。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-2021-36471
https://www.cnvd.org.cn/flaw/show/CNVD-2021-36470
https://www.cnvd.org.cn/flaw/show/CNVD-2021-36469
https://www.cnvd.org.cn/flaw/show/CNVD-2021-36468
https://www.cnvd.org.cn/flaw/show/CNVD-2021-36474
https://www.cnvd.org.cn/flaw/show/CNVD-2021-36473
https://www.cnvd.org.cn/flaw/show/CNVD-2021-36472
https://www.cnvd.org.cn/flaw/show/CNVD-2021-36478

3、Jetbrains 产品安全漏洞

JetBrains IntelliJ IDEA 是捷克 JetBrains 公司的一套适用于 Java 语言的集成开发环境。JetBrains TeamCity 是捷克 JetBrains 公司的一套分布式构建管理和持续集成工具。该工具提供持续单元测试、代码质量分析和构建问题分析报告等功能。JetBrains Code With Me 是捷克 JetBrains 公司的一款可为 IntelliJ IDE 提供代码协同编辑的插件应用。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，执行客户端代码等。

CNVD 收录的相关漏洞包括：JetBrains IntelliJ IDEA 拒绝服务漏洞、JetBrains TeamCity 服务端请求伪造漏洞、JetBrains TeamCity 跨站脚本漏洞（CNVD-2021-35241）、JetBrains IntelliJ IDEA 外部实体注入漏洞、JetBrains TeamCity 远程代码执行漏洞、JetBrains TeamCity 信任管理问题漏洞（CNVD-2021-35238）、JetBrains IntelliJ IDEA 本地代码执行漏洞、JetBrains Code With Me 代码执行漏洞。其中，“JetBrains TeamCity 远程代码执行漏洞”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-2021-34990
https://www.cnvd.org.cn/flaw/show/CNVD-2021-35237
https://www.cnvd.org.cn/flaw/show/CNVD-2021-35241
https://www.cnvd.org.cn/flaw/show/CNVD-2021-35240
https://www.cnvd.org.cn/flaw/show/CNVD-2021-35239

https://www.cnvd.org.cn/flaw/show/CNVD-2021-35238

https://www.cnvd.org.cn/flaw/show/CNVD-2021-35242

https://www.cnvd.org.cn/flaw/show/CNVD-2021-35611

4、WordPress 产品安全漏洞

WordPress 是 WordPress（Wordpress）基金会的一套使用 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 WP Customer Reviews 是（Wordpress）开源的一个应用插件。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞发起跨站脚本攻击，导致远程代码执行等。

CNVD 收录的相关漏洞包括：WordPress Redirection for Contact Form 7 Plugin 访问控制不当漏洞（CNVD-2021-36044）、WordPress Redirection for Contact Form 7 Plugin PHP 对象注入漏洞、WordPress Business Directory Plugin 远程代码执行漏洞、WordPress Ultimate Maps by Supsystic Plugin 跨站脚本漏洞、WordPress Elements Kit Lite and Elements Kit Pro Plugin 跨站脚本漏洞、Wordpress WP Customer Reviews 跨站脚本漏洞、WordPress plugin 跨站脚本漏洞（CNVD-2021-36524、CNVD-2021-36523）。其中，“WordPress Redirection for Contact Form 7 Plugin 访问控制不当漏洞（CNVD-2021-36044）”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-2021-36044

https://www.cnvd.org.cn/flaw/show/CNVD-2021-36048

https://www.cnvd.org.cn/flaw/show/CNVD-2021-36054

https://www.cnvd.org.cn/flaw/show/CNVD-2021-36059

https://www.cnvd.org.cn/flaw/show/CNVD-2021-36067

https://www.cnvd.org.cn/flaw/show/CNVD-2021-36073

https://www.cnvd.org.cn/flaw/show/CNVD-2021-36524

https://www.cnvd.org.cn/flaw/show/CNVD-2021-36523

5、OpenClinic GA 权限提升漏洞

OpenClinic GA 是一套开源的医院信息管理系统。该系统支持财务管理、临床管理和实验室管理等功能。本周，OpenClinic GA 被披露存在权限提升漏洞。该漏洞源于默认权限错误。攻击者可通过覆盖二进制文件利用该漏洞导致特权升级。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-2021-35006

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	修复方式

		评级	
CNVD-2021-35247	D-Link DAP-1880AC 访问控制错误漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.dlink-jp.com/support/release/jvnvu92898656_dap-1880ac.html
CNVD-2021-35498	vBulletin 不正确访问控制漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://forum.vbulletin.com/forum/vbulletin-announcements/vbulletin-announcements_aa/4440032-vbulletin-5-6-1-security-patch-level-1
CNVD-2021-35502	Adobe Genuine Integrity Service 不安全文件权限漏洞	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/integrity_service/apsb20-12.html
CNVD-2021-35507	Open Design Alliance Drawings SDK 越界写入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.opendesign.com/security-advisories
CNVD-2021-35614	HPE Edgeline Infrastructure Manager 授权问题漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbgn04124en_us
CNVD-2021-35620	Micro Focus Application Performance Management 代码执行漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://softwaresupport.softwaregrp.com/doc/KM03806501
CNVD-2021-36021	TP-Link TL-WR802N（US）和 Archer_C50v5_US 缓冲区溢出漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.tp-link.com/us/support/download/tl-wr802n/#Firmware
CNVD-2021-36017	Dell SRM 和 SMR 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://www.dell.com/support/kbdoc/en-us/000184753/dsa-2021-054-dell-emc-srm-and-dell-emc-storage-monitoring-and-reporting-smr-security-update-for-multiple-vulnerabilities
CNVD-2021-36103	Omron CX-One 缓冲区溢出漏洞（CNVD-2021-36103）	高	目前厂商已发布升级补丁以修复漏洞，详情请关注厂商主页：https://www.omron.com/global/en/
CNVD-2021-	Moxa Camera VPort 06EC-2	高	目前厂商已发布升级补丁以修复漏

36216	V 存在未明漏洞（CNVD-2021-36216）		洞，补丁获取链接：https://www.moxa.com/en/support/product-support/security-advisory/vport-06ec-2v-series-ip-cameras-vulnerabilities

小结：本周，Google 产品被披露存在多个漏洞，攻击者可利用漏洞通过特制的 HTML 页面执行域欺骗，绕过安全限制，执行任意代码或造成拒绝服务等。此外，Foxit、Jetbrains、WordPress 等多款产品被披露存在多个漏洞，攻击者可利用漏洞发起跨站脚本攻击，获取敏感信息，执行客户端代码等。另外，OpenClinic GA 被披露存在权限提升漏洞。攻击者可通过覆盖二进制文件利用该漏洞导致特权升级。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、PHPGurukul Online Book Store 任意文件上传漏洞

验证描述

PHPGurukul Online Book Store 是一套基于 PHP 的在线书店网站系统。

PHPGurukul Online Book Store v1.0 版本中的 admin_add.php 存在任意文件上传漏洞。攻击者可利用该漏洞实现远程代码执行。

验证信息

POC 链接：https://github.com/projectworldsofficial/online-book-store-project-in-php/issues/15

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2021-35005

信息提供者

卫士通信息产业股份有限公司

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. 对象注入漏洞影响 WordPress 版本 3.7 至 5.7.1

PHP 对象注入是一个应用程序级别的漏洞，可以使攻击者执行不同种类的恶意攻击，例如代码注入，SQL 注入，路径遍历和应用程序拒绝服务。

参考链接：https://blog.sucuri.net/2021/05/object-injection-vulnerability-affects-wordpress-versions-3-7-to-5-7-1.html?web_view=true

2. 研究人员揭示存在 54 年的通用图灵机零日漏洞，可用于执行任意代码

瑞典的一位计算机科学家在 Marvin Minsky 设计的通用图灵机（Universal Turing Machine）中发现了一个 0day 漏洞，允许任意代码执行。

参考链接：https://www.cnbeta.com/articles/tech/1128909.htm

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