国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2021 年 09 月 06 日-2021 年 09 月 12 日 **2021 年第 36 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 562 个，其中高危漏洞 144 个、中危漏洞 377 个、低危漏洞 41 个。漏洞平均分值为 5.72。本周收录的漏洞中，涉及 0day 漏洞 397 个（占 71%），其中互联网上出现“WordPress SP Project And Document 远程代码执行漏洞、MIK.starlight 输入验证错误漏洞”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原创漏洞总数 6218 个，与上周（12712 个）环比减少 51%。

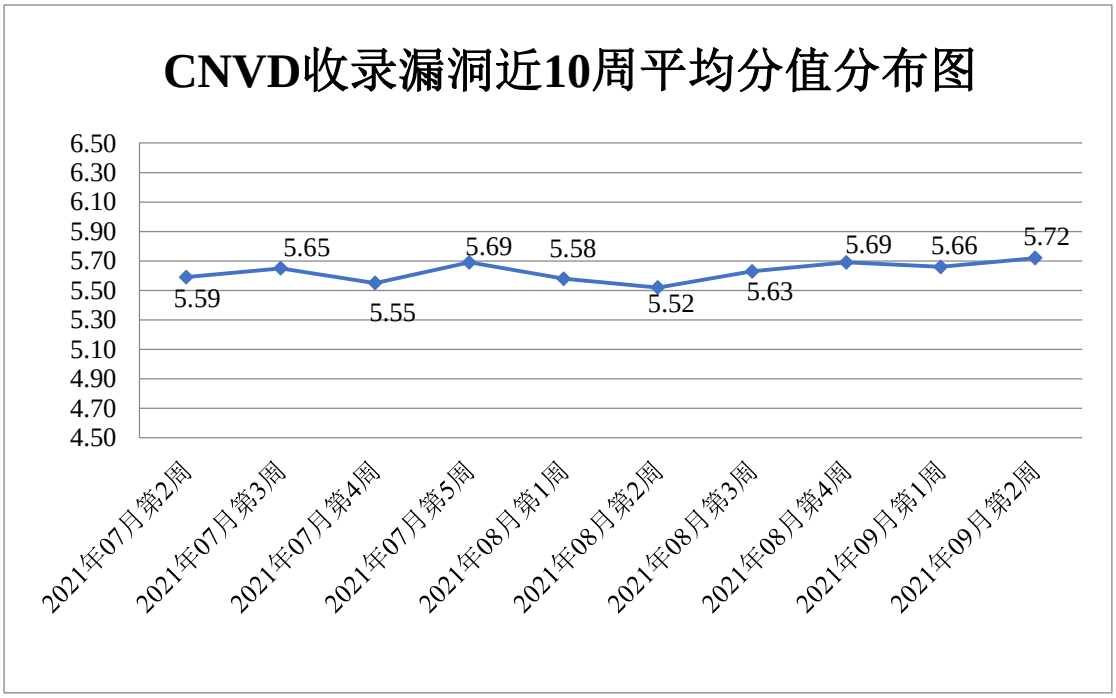

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 20 起，向基础电信企业通报漏洞事件 40 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 429 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 49 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 40 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：

紫光软件系统有限公司、淄博闪灵网络科技有限公司、株洲汉诺网络科技有限公司、珠海新华通软件股份有限公司、珠海玖时光科技有限公司、珠海高凌信息科技股份有限公司、重庆远秋科技有限公司、众阳健康科技集团有限公司、中煤（西安）地下空间科技发展有限公司、中国电信股份有限公司上海分公司、郑州方果电子科技有限公司、镇江市云优网络科技有限公司、浙江环鑫信息技术有限公司、长沙德尚网络科技有限公司、友讯电子设备（上海）有限公司、徐州亿优网架钢结构工程有限公司、新天科技股份有限公司、小米科技有限责任公司、夏普商贸（中国）有限公司、希捷科技有限公司、西安众邦网络科技有限公司、西安交大捷普网络科技有限公司、西安嘉客信息科技有限责任公司、武汉微问网络科技有限公司、无锡医库软件科技有限公司、统信软件技术有限公司、索尼（中国）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、四川迅游网络科技股份有限公司、世邦通信股份有限公司、神州数码控股有限公司、深圳市唯德科创信息有限公司、深圳市万网博通科技有限公司、深圳市腾讯计算机系统有限公司、深圳市模拟科技有限公司、深圳市米亚印乐科技有限公司、深圳市美科星通信技术有限公司、深圳市磊科实业有限公司、深圳齐心好视通云计算有限公司、上海卓卓网络科技有限公司、上海易教科技股份有限公司、上海新网程信息技术股份有限公司、上海明牛云科技有限公司、上海巨子信息科技有限公司、上海井星信息科技有限公司、上海汉得信息技术股份有限公司、上海泛微网络科技股份有限公司、上海顶想信息科技有限公司、山东科德电子有限公司、山东金钟科技集团股份有限公司、厦门四信通信科技有限公司、任子行网络技术股份有限公司、普生(中国)有限公司、邳州天目网络科技有限公司、宁波华硕网络服务有限公司、南宁比优网络科技有限公司、南京同享网络科技有限公司、南京龙媒网络科技有限公司、茉柏枘（上海）软件科技有限公司、迈普通信技术股份有限公司、猎豹移动公司、联奕科技股份有限公司、乐元素科技（北京）股份有限公司、朗坤智慧科技股份有限公司、酷艺文化科技发展有限公司、江苏卓易信息科技股份有限公司、江苏汇文软件有限公司、济南步天网络技术有限公司、济南爱程网络科技有限公司、霍尼韦尔（中国）有限公司、惠普贸易（上海）有限公司、华平信息技术股份有限公司、华大半导体有限公司、湖南壹拾捌号网络技术有限公司、湖南青果软件有限公司、湖北索拓星蓝科技有限公司、湖北点点点科技有限公司、黑龙江立高科技股份有限公司、杭州圣乔科技有限公司、杭州宏服软件有限公司、杭州海康威

视数字技术股份有限公司、杭州冠航科技有限公司、杭州飞畅科技有限公司、汉王科技股份有限公司、海南赞赞网络科技有限公司、广州视睿电子科技有限公司、广州市小弹壳网络科技有限公司、广州市国万电子科技有限公司、广州市成格信息技术有限公司、广州市奥威亚电子科技有限公司、广州齐博网络科技有限公司、广州本盈计算机科技有限公司、广州安网通信技术有限公司、广联达科技股份有限公司、广东力拓网络科技有限公司、高通企业管理（上海）有限公司、福州网钛软件科技有限公司、福建福昕软件开发股份有限公司、帆软软件有限公司、大汉软件股份有限公司、程景（北京）科技有限公司、成都亿友科技有限公司、成都万江港利科技有限公司、成都佳发安泰教育科技股份有限公司、畅捷通信息技术股份有限公司、北京致远互联软件股份有限公司、北京兆易创新科技股份有限公司、北京映翰通网络技术股份有限公司、北京医百科技有限公司、北京星网锐捷网络技术有限公司、北京网御星云信息技术有限公司、北京通达信科科技有限公司、北京时空智友科技有限公司、北京神州数码云科信息技术有限公司、北京平凯星辰科技发展有限公司、北京派网软件有限公司、北京宽广智通信息技术有限公司、北京快手科技有限公司、北京九思协同软件有限公司、北京江民新科技术有限公司、北京火木科技有限公司、北京灯果网络科技有限公司、北京爱奇艺科技有限公司、台达集团、上海布雷德网络科技、桂林崇胜网络科技、上海程江科技中心、优效软件工作室、帝国软件、捷微、信呼、无忧网络、百家 CMS 微商城、鱼跃 CMS、狂雨小说 cms、WMCMS 团队、MIP 建站系统、ZZCMS、xycms、ucms、SEMCMS、RTCMS、phpaaCMS、Oracle、Nitro Software、NetSarang、Monstra、Lexmark、ExtractNow、Classcms、catfishcms、Belkin International,Inc、Apache 和 AKCMS。

本周，CNVD 发布了《关于 Microsoft MSHTML 存在远程代码执行漏洞的安全公告》。详情参见 CNVD 网站公告内容。

https://www.cnvd.org.cn/webinfo/show/6821

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，阿里云计算有限公司、哈尔滨安天科技集团股份有限公司、厦门服云信息科技有限公司、新华三技术有限公司、北京神州绿盟科技有限公司等单位报送公开收集的漏洞数量较多。山东云天安全技术有限公司、北京华云安信息技术有限公司、南京众智维信息科技有限公司、河南灵创电子科技有限公司、内蒙古洞明科技有限公司、亚信科技（成都）有限公司、北京信联科汇科技有限公司、北京安帝科技有限公司、内蒙古云科数据服务股份有限公司、安徽长泰科技有限公司、广东蓝爵网络安全技术股份有限公司、河南信安世纪科技有限公司、北京远禾科技有限公司、平安银河实验室、浙江木链物联网科技有限公司、上海纽盾科技股份有限公司、山东泽鹿安全技术有限公司、北京云科安信科技有限公司（Seraph 安全实验室）、北京天地和

兴科技有限公司、星云博创科技有限公司、泰山信息科技有限公司、杭州美创科技有限公司、阿里巴巴网络技术有限公司、广州安亿信软件科技有限公司、北京惠而特科技有限公司、河南天祺信息安全技术有限公司、重庆都会信息科技有限公司、博智安全科技股份有限公司、浙江国利网安科技有限公司、深圳市魔方安全科技有限公司、北京山石网科信息技术有限公司、武汉绿色网络信息服务有限责任公司、南京树安信息技术有限公司、杭州海康威视数字技术股份有限公司、汇安信息科技有限公司、北京顶象技术有限公司、杭州安信检测技术有限公司、贵州多彩宝互联网服务有限公司、山石网科通信技术股份有限公司、赛尔网络有限公司山东分公司其他个人白帽子向CNVD提交了6218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）和上海交大向CNVD共享的白帽子报送的3755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）	2292	2292
奇安信网神（补天平台）	1073	1073
阿里云计算有限公司	402	0
上海交大	390	390
哈尔滨安天科技集团股份有限公司	252	0
厦门服云信息科技有限公司	240	0
新华三技术有限公司	219	0
北京神州绿盟科技有限公司	211	5
北京数字观星科技有限公司	186	0
北京天融信网络安全技术有限公司	180	11
恒安嘉新（北京）科技股份公司	128	0
深信服科技股份有限公司	95	0
北京启明星辰信息安全技术有限公司	90	28

华为技术有限公司	85	0
远江盛邦（北京）网络安全科技股份有限公司	65	65
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)	53	0
北京奇虎科技有限公司	26	0
北京长亭科技有限公司	7	7
南京联成科技发展股份有限公司	6	6
北京知道创宇信息技术有限公司	4	1
杭州安恒信息技术股份有限公司	4	4
西安四叶草信息技术有限公司	2	2
内蒙古奥创科技有限公司	1	1
北京智游网安科技有限公司	1	1
山东云天安全技术有限公司	335	335
北京华云安信息技术有限公司	180	180
南京众智维信息科技有限公司	119	119
联想全球安全实验室	106	0
河南灵创电子科技有限公司	103	103
内蒙古洞明科技有限	54	54

公司		
亚信科技（成都）有限公司	36	1
北京信联科汇科技有限公司	35	35
北京安帝科技有限公司	31	31
杭州迪普科技股份有限公司	30	0
内蒙古云科数据服务股份有限公司	28	28
安徽长泰科技有限公司	27	27
广东蓝爵网络安全技术股份有限公司	26	26
中国电信股份有限公司网络安全产品运营中心	20	0
河南信安世纪科技有限公司	15	15
北京远禾科技有限公司	13	13
平安银河实验室	10	10
浙江木链物联网科技有限公司	10	10
上海纽盾科技股份有限公司	9	9
山东泽鹿安全技术有限公司	9	9
北京云科安信科技有限公司（Seraph 安全实验室）	8	8
北京天地和兴科技有限公司	8	8

星云博创科技有限公司	6	6
泰山信息科技有限公司	5	5
杭州美创科技有限公司	4	4
阿里巴巴网络技术有限公司	4	4
广州安亿信软件科技有限公司	2	2
北京惠而特科技有限公司	2	2
河南天祺信息安全技术有限公司	2	2
重庆都会信息科技有限公司	2	2
博智安全科技股份有限公司	2	2
浙江国利网安科技有限公司	2	2
深圳市魔方安全科技有限公司	1	1
北京山石网科信息技术有限公司	1	1
武汉绿色网络信息服务有限责任公司	1	1
南京树安信息技术有限公司	1	1
杭州海康威视数字技术股份有限公司	1	1
汇安信息科技有限公司	1	1
北京顶象技术有限公司	1	1

杭州安信检测技术有限公司	1	1
贵州多彩宝互联网服务有限公司	1	1
山石网科通信技术股份有限公司	1	1
赛尔网络有限公司山东分公司	1	1
CNCERT 宁夏分中心	2	2
CNCERT 河北分中心	1	1
CNCERT 贵州分中心	1	1
CNCERT 河南分中心	1	1
个人	1264	1264
报送总计	8535	6218

本周漏洞按类型和厂商统计

本周，CNVD 收录了 562 个漏洞。WEB 应用 241 个，应用程序 201 个，网络设备（交换机、路由器等网络端设备）69 个，操作系统 26 个，安全产品 14 个，智能设备（物联网终端设备）漏洞 10 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
WEB 应用	241
应用程序	201
网络设备（交换机、路由器等网络端设备）	69
操作系统	26
安全产品	14
智能设备（物联网终端设备）漏洞	10
数据库	1

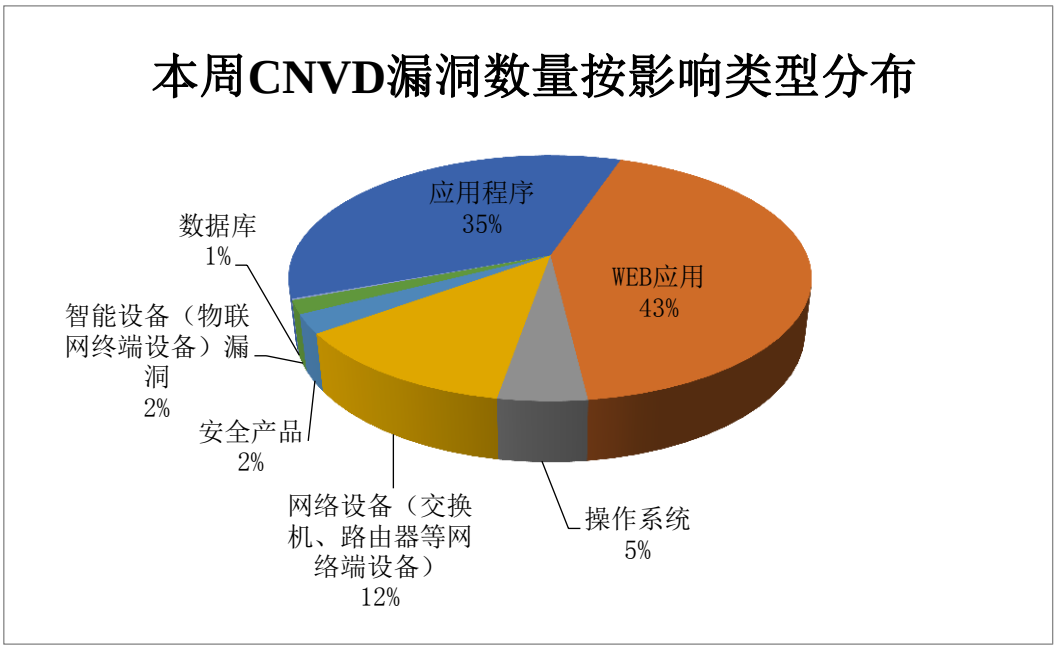

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 SWFTools、Microsoft、libredwg 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	SWFTools	37	7%
2	Microsoft	36	6%
3	libredwg	27	5%
4	爱青檬 CMS	16	3%
5	D-Link	19	3%
6	Cisco	14	2%
7	Apache	12	2%
8	Adobe	10	2%
9	Bento4	9	2%
10	其他	382	68%

本周行业漏洞收录情况

本周，CNVD 收录了 52 个电信行业漏洞，24 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，“Delta Electronics DOPSoft 越界读取漏洞、Ypsomed mylife App 信任管理问题漏洞、Cisco IOS XR Software 命令注入漏洞”等漏洞的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/

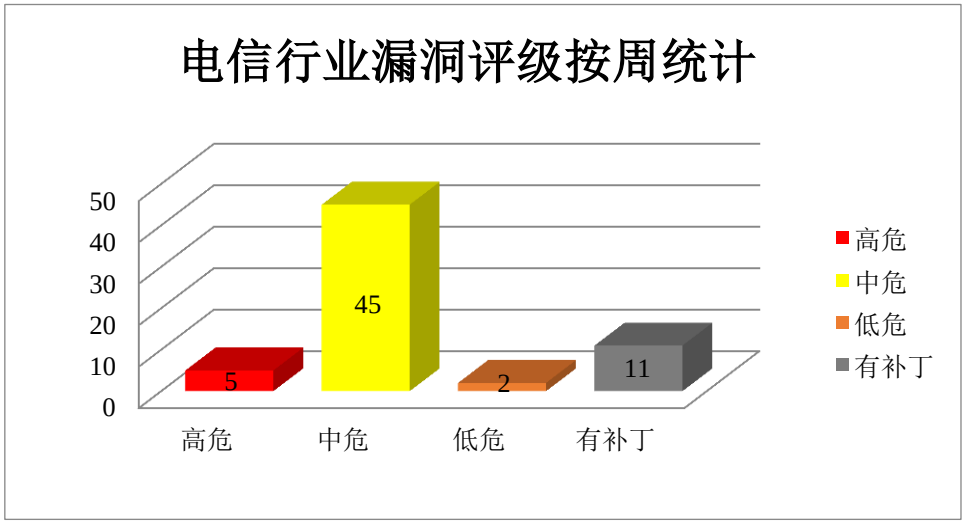

图 3 电信行业漏洞统计

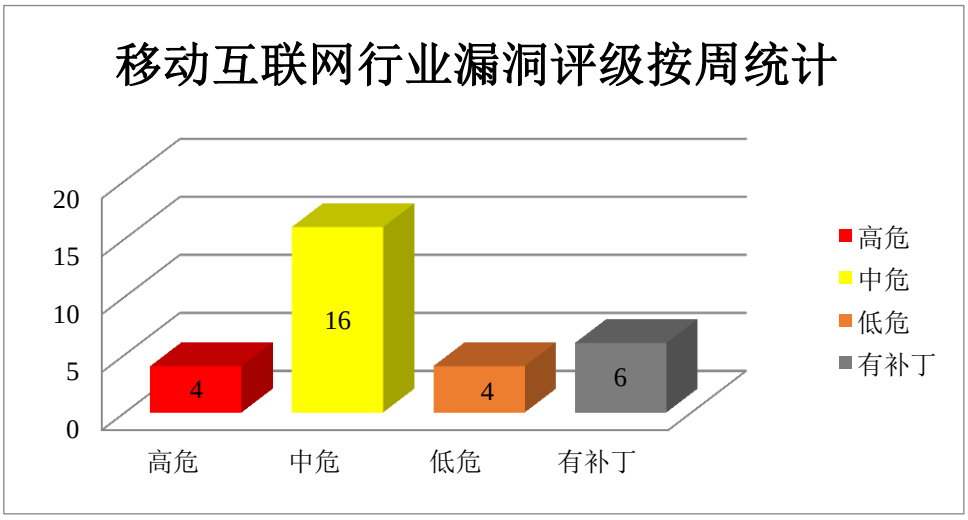

图 4 移动互联网行业漏洞统计

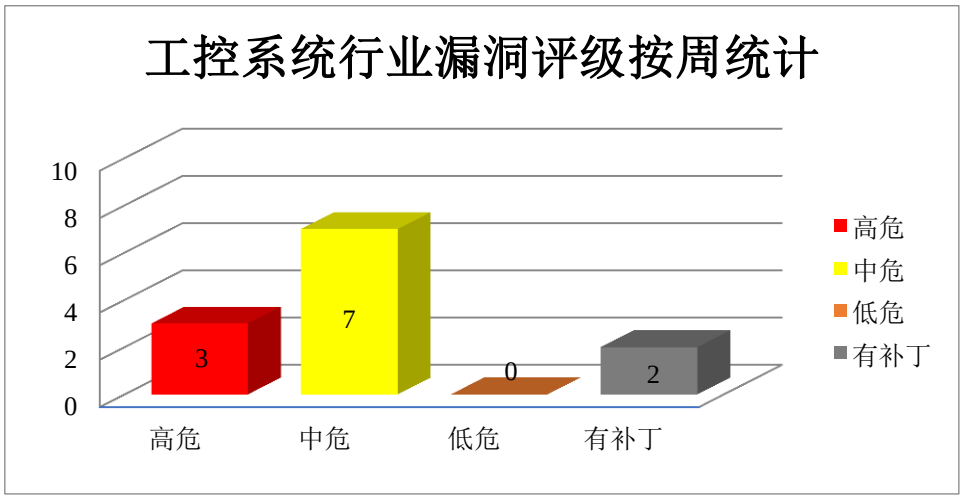

图 5 工控系统行业漏洞统计

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、 Microsoft 产品安全漏洞

Microsoft Windows 是一套个人设备使用的操作系统。Microsoft Windows Server 是一套服务器操作系统。MSHTML（又称为 Trident）是微软旗下的 Internet Explorer 浏览器引擎，虽然 MHTML 主要用于已被弃用的 Internet Explorer 浏览器，但该组件也用于 Office 应用程序，以在 Word、Excel 或 PowerPoint 文档中呈现 Web 托管的内容。本周，上述产品被披露存在权限提升和远程执行代码漏洞，攻击者可利用漏洞实现权限提升，执行任意代码。

CNVD 收录的相关漏洞包括：Microsoft Windows/Windows Server 权限提升漏洞（CNVD-2021-68742、CNVD-2021-68741、CNVD-2021-68743、CNVD-2021-68748、CNVD-2021-68749）、Microsoft MSHTML 远程代码执行漏洞、Microsoft HEVC Video Extensions 远程代码执行漏洞（CNVD-2021-70142、CNVD-2021-70141）。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-2021-68742

https://www.cnvd.org.cn/flaw/show/CNVD-2021-68741

https://www.cnvd.org.cn/flaw/show/CNVD-2021-68743

https://www.cnvd.org.cn/flaw/show/CNVD-2021-68748

https://www.cnvd.org.cn/flaw/show/CNVD-2021-68749

https://www.cnvd.org.cn/flaw/show/CNVD-2021-69088

https://www.cnvd.org.cn/flaw/show/CNVD-2021-70142

https://www.cnvd.org.cn/flaw/show/CNVD-2021-70141

2、 Cisco 产品安全漏洞

Cisco NX-OS Software 是美国思科（Cisco）公司的一套交换机使用的数据中心级操作系统软件。Cisco Application Policy Infrastructure Controller（APIC）是美国思科（Cisco）公司的一款自动化的基础架构部署和治理解决方案。Cisco Evolved Programmable Network Manager 是美国思科（Cisco）公司的一套网络管理解决方案。Cisco SD-WAN Solution 是 Cisco 的一套网络扩展解决方案，vManage 是其中的控制台。本周，上述产品被披露存在多个漏洞，攻击者可利用该漏洞获取敏感信息，提升权限，在受影响的设备上读取或写入任意文件，导致拒绝服务攻击等。

CNVD 收录的相关漏洞包括：Cisco NX-OS Software 拒绝服务漏洞（CNVD-2021-68723、CNVD-2021-68721、CNVD-2021-68727）、Cisco Application Policy Infrastructure Controller 任意文件读写漏洞、Cisco Application Policy Infrastructure Controller 权

限提升漏洞（CNVD-2021-68725、CNVD-2021-68724）、Cisco Evolved Programmable Network Manager 信息泄露漏洞、Cisco SD-WAN vManage Software 信息泄露漏洞（CNVD-2021-68733）。其中，“Cisco Application Policy Infrastructure Controller 权限提升漏洞（CNVD-2021-68725、CNVD-2021-68724）”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-2021-68723
https://www.cnvd.org.cn/flaw/show/CNVD-2021-68722
https://www.cnvd.org.cn/flaw/show/CNVD-2021-68721
https://www.cnvd.org.cn/flaw/show/CNVD-2021-68727
https://www.cnvd.org.cn/flaw/show/CNVD-2021-68725
https://www.cnvd.org.cn/flaw/show/CNVD-2021-68724
https://www.cnvd.org.cn/flaw/show/CNVD-2021-68731
https://www.cnvd.org.cn/flaw/show/CNVD-2021-68733

3、 Apache 产品安全漏洞

Apache jUDDI 是一个服务于 WebServices 的 UDDI 的 java 实现开源包。Apache CXF 是美国阿帕奇（Apache）基金会的一个开源的 Web 服务框架。该框架支持多种 Web 服务标准、多种前端编程 API 等。Apache ServiceComb Service-Center 是 Apache 基金会的一个基于 Restful 的服务注册中心，提供微服务发现和微服务管理。Apache Pulsar 是美国阿帕奇（Apache）基金会的一个用于云环境种，集消息、存储、轻量化函数式计算为一体的分布式消息流平台。Apache HTTP Server 是美国阿帕奇（Apache）基金会的一款开源网页服务器。Apache Zeppelin 是美国阿帕奇（Apache）基金会的一款基于 Web 的开源笔记本应用程序，该程序支持交互式数据分析和协作文档。本周，上述产品被披露存在多个漏洞，攻击者可利用该漏洞绕过身份验证过程，注入恶意脚本，导致拒绝服务攻击。

CNVD 收录的相关漏洞包括：Apache jUDDI 代码问题漏洞、Apache CXF 资源管理错误漏洞（CNVD-2021-70100）、Apache ServiceComb Service-Center 路径遍历漏洞、Apache Pulsar 数据伪造问题漏洞、Apache HTTP Server 拒绝服务漏洞（CNVD-2021-70103）、Apache Zeppelin 跨站脚本漏洞、Apache Zeppelin 命令注入漏洞、Apache Zeppelin 身份验证绕过漏洞。其中，“Apache Pulsar 数据伪造问题漏洞、Apache HTTP Server 拒绝服务漏洞（CNVD-2021-70103）、Apache Zeppelin 命令注入漏洞” 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-2021-69948
https://www.cnvd.org.cn/flaw/show/CNVD-2021-70100

https://www.cnvd.org.cn/flaw/show/CNVD-2021-70099

https://www.cnvd.org.cn/flaw/show/CNVD-2021-70104

https://www.cnvd.org.cn/flaw/show/CNVD-2021-70103

https://www.cnvd.org.cn/flaw/show/CNVD-2021-70121

https://www.cnvd.org.cn/flaw/show/CNVD-2021-70120

https://www.cnvd.org.cn/flaw/show/CNVD-2021-70119

4、Adobe 产品安全漏洞

Adobe Acrobat 是由 Adobe 公司开发的一款 PDF 编辑软件。Adobe Reader（也被称为 Acrobat Reader)是由 Adobe 公司开发的一款 PDF 文件阅读软件。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞获取敏感信息，执行任意代码等。

CNVD 收录的相关漏洞包括：Adobe Acrobat/Reader 越界写入漏洞（CNVD-2021-70144）、Adobe Acrobat/Reader 类型混淆漏洞（CNVD-2021-70147）、Adobe Acrobat/Reader 释放后重用漏洞（CNVD-2021-70146、CNVD-2021-70145、CNVD-2021-70148）、Adobe Acrobat/Reader 越界读取漏洞（CNVD-2021-70151、CNVD-2021-70152、CNVD-2021-70149）。其中，“Adobe Acrobat/Reader 释放后重用漏洞（CNVD-2021-70145）、Adobe Acrobat/Reader 路径遍历漏洞（CNVD-2021-70149）”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-2021-70144

https://www.cnvd.org.cn/flaw/show/CNVD-2021-70147

https://www.cnvd.org.cn/flaw/show/CNVD-2021-70146

https://www.cnvd.org.cn/flaw/show/CNVD-2021-70145

https://www.cnvd.org.cn/flaw/show/CNVD-2021-70151

https://www.cnvd.org.cn/flaw/show/CNVD-2021-70149

https://www.cnvd.org.cn/flaw/show/CNVD-2021-70148

https://www.cnvd.org.cn/flaw/show/CNVD-2021-70152

5、DIAEnergie 跨站请求伪造漏洞

DIAEnergie 是 Delta Electronics 推出的一款工业能源管理系统。本周，DIAEnergie 被披露存在跨站请求伪造漏洞。攻击者可利用该漏洞执行未授权操作。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-2021-68442

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-2021-70158	Delta Electronics DIAScreen 类型混淆漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://diastudio.deltaww.com/home/downloads?sec=download
CNVD-2021-70112	Fortinet FortiWeb 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://www.auscert.org.au/bulletins/ESB-2021.3006
CNVD-2021-68448	ProLink PRC2402M 命令注入漏洞	高	目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载：https://www.ayrx.me/prolink-prc2402m-multiple-vulnerabilities/#ledonoff-command-injection
CNVD-2021-68757	HealthNode Hospital Management System SQL 注入漏洞	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://github.com/kishan0725/Hospital-Management-System
CNVD-2021-69950	IBM Power HMC 权限提升漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.ibm.com/
CNVD-2021-70089	ZTE ZXV10 M910 代码问题漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://www.zte.com.cn/china/support
CNVD-2021-70109	Nextcloud 信息泄露漏洞（CNVD-2021-70109）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://github.com/nextcloud/security-advisories/security/advisories/GHSA-pxhh-954f-8w7w
CNVD-2021-70111	Fortinet FortiWeb 缓冲区溢出漏洞（CNVD-2021-70111）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://www.auscert.org.au/bulletins/ESB-2021.3006
CNVD-2021-70150	Adobe Acrobat/Reader 路径遍历漏洞	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/acrobat/apsb21-51.html
CNVD-2021-70157	Delta Electronics DIAScreen 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://diastudio.deltaww.com/home/downloads?sec=download

小结：本周，Microsoft 产品被披露存在权限提升和远程执行代码漏洞，攻击者可利用漏洞实现权限提升，执行任意代码。此外，Cisco、Apache、Adobe 等多款产品被披露存在多个漏洞，攻击者可利用该漏洞绕过身份验证过程，获取敏感信息，注入恶意脚本，提升权限，在受影响的设备上读取或写入任意文件，执行任意代码，导致拒绝服务攻击等。另外，DIAEnergie 被披露存在跨站请求伪造漏洞。攻击者可利用该漏洞执行未授权操作。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、WordPress SP Project And Document 远程代码执行漏洞

验证描述

WordPress 是基于 PHP 语言开发的博客平台，可以用于在支持 PHP 和 MySQL 数据库的服务器上架设网站，也可当做一个内容管理系统（CMS）。

WordPress SP Project And Document 存在远程代码执行漏洞，攻击者可利用该漏洞执行任意代码。

验证信息

POC 链接：https://cxsecurity.com/issue/WLB-2021070159

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2021-70161

信息提供者

深信服科技股份有限公司

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. 攻击者利用 Confluence 漏洞，入侵 Jenkins 项目服务器

Jenkins 服务器背后开发团队披露了一个安全漏洞，该漏洞是一个 OGNL（对象导航图语言）注入问题。经过身份验证的攻击者可以利用该漏洞，在 Confluence 服务器和数据中心执行任意代码，攻击者在一台服务器上部署了加密挖矿工具。

参考链接：https://www.freebuf.com/news/287876.html

2. 三星 Galaxy Z Flip3 5G 的小窗存在漏洞：可显示完整 App，且无需 root

XDA 成员 CarudiBu 发现了一个漏洞，可以让 Galaxy Z Flip 3 的小窗加载自定义小部件，从而间接运行完整 App。

参考链接：https://finance.sina.com.cn/tech/2021-09-07/doc-iktzqtyt4496150.shtml

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