国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2021 年 11 月 29 日-2021 年 12 月 05 日 **2021 年第 48 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 553 个，其中高危漏洞 166 个、中危漏洞 326 个、低危漏洞 61 个。漏洞平均分值为 5.79。本周收录的漏洞中，涉及 0day 漏洞 300 个（占 54%），其中互联网上出现“Libmobi 缓冲区溢出漏洞、Phpjabbers Appointment Scheduler 跨站脚本漏洞”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 10359 个，与上周（4773 个）环比增加 117%。

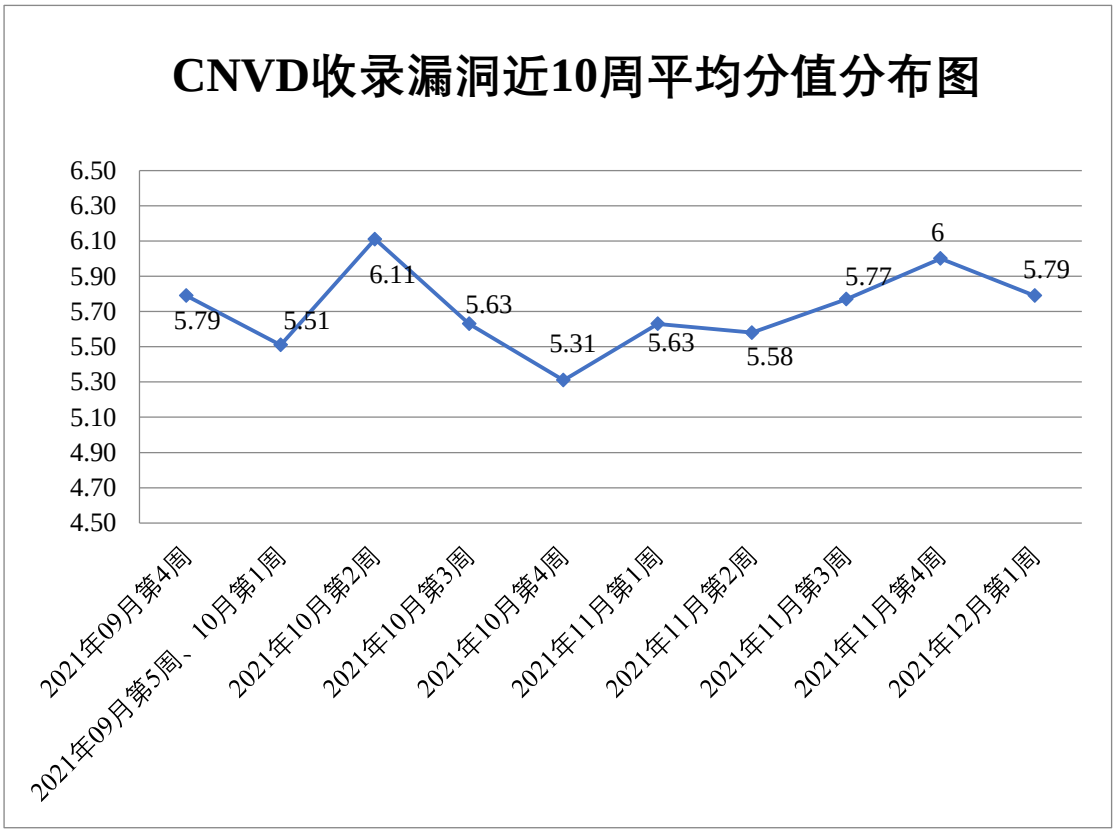

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 19 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 719 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 87 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 74 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：

淄博闪灵网络科技有限公司、中铁信托有限责任公司、中科博华信息科技有限公司、中国电信集团公司、中版行知（广州）数字传媒有限公司、友讯电子设备（上海）有限公司、兄弟（中国）商业有限公司、校无忧科技网络公司、西安凤巢网络科技有限公司、武汉舜通智能科技有限公司、武汉烽火众智数字技术有限责任公司、微软（中国）有限公司、网宿科技股份有限公司、天津神州浩天科技有限公司、泰华智慧产业集团股份有限公司、台达电子企业管理（上海）有限公司、松下电器（中国）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、四川云图信息技术有限公司、思科系统（中国）网络技术有限公司、数字化（广州）科技有限公司、石家庄和嘉科技有限公司、深圳市圆梦云科技有限公司、深圳市睿炽科技有限公司、深圳市蓝凌软件股份有限公司、深圳市捷视飞通科技股份有限公司、深圳市杰成合力科技有限公司、深圳市吉祥腾达科技有限公司、深圳市合信自动化技术有限公司、深圳市皓峰通讯技术有限公司、深圳华望技术有限公司、上海亿速网络科技有限公司、上海软众网络科技有限公司、上海牛迈网络科技有限公司、上海汇尼信息科技有限公司、上海寰创通信科技股份有限公司、上海二三四五移动科技有限公司、上海宝信软件股份有限公司、山东金钟科技集团股份有限公司、厦门科汛软件有限公司、南京悠珀网络科技有限公司、六安校无忧信息科技有限公司、江苏图星软件科技有限责任公司、佳能（中国）有限公司、济南博观智能科技有限公司、淮南市银泰软件科技有限公司、湖南壹拾捌号网络技术有限公司、湖南人才就业社保信息报社有限责任公司、湖南康通电子股份有限公司、河南恩熙信息技术有限公司、合肥奇乐网络科技有限公司、合肥明信软件技术有限公司、杭州中宝科技有限公司、杭州三汇信息工程有限公司、杭州阔知网络科技有限公司、杭州冠航科技有限公司、汉王科技股份有限公司、哈尔滨新中新电子股份有限公司、广州智雄软件有限公司、广州齐博网络科技有限公司、广州酷狗计算机科技有限公司、广联达科技股份有限公司、高新兴科技集团股份有限公司、飞利浦（中国）投资有限公司、成都友加畅捷科技有限公司、成都零起飞科技有限公司、贝尔金国际有限公司、北京中创视讯科技有限公司、北京智敏科技发展有限公司、北京致远互联软件股份有限公司、北京育网阳光科技有限公司、北京雪迪龙科技股份有限公司、北京星网锐捷网络技术有限公司、北京五指互联

科技有限公司、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、北京勤云科技发展有限公司、北京派网软件有限公司、北京魔方恒久软件有限公司、北京汉邦高科数字技术股份有限公司、北京奥腾岩石科技有限公司、和利时集团、宁海县人民政府办公室、国家铁塔工程安全质量监督检验中心、施耐德（Schneider Electric）、百度安全应急响应中心、无忧网络、网展科技、中興保全科技、巡云轻论坛系统、信呼、ZZCMS、wolfSSL Inc.、The Apache Software Foundation、JeePlus、Iceni Technology、HadSky、ElasticSearch、Code Industry Ltd 和 ClassCMS。

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、北京神州绿盟科技有限公司、哈尔滨安天科技集团股份有限公司、新华三技术有限公司、北京数字观星科技有限公司等单位报送公开收集的漏洞数量较多。北京信联科汇科技有限公司、广东蓝爵网络安全技术股份有限公司、贵州多彩宝互联网服务有限公司、山东新潮信息技术有限公司、南京树安信息技术有限公司、重庆都会信息科技、安徽长泰科技有限公司、长春嘉诚信息技术股份有限公司、北京安帝科技有限公司、杭州海康威视数字技术股份有限公司、星云博创科技有限公司、杭州迪普科技股份有限公司、北京远禾科技有限公司、河南信安世纪科技有限公司、北京威努特技术有限公司、亚信科技（成都）有限公司、京东云安全、河南灵创电子科技有限公司、上海纽盾科技股份有限公司、山东云天安全技术有限公司、福建省海峡信息技术有限公司、博智安全科技股份有限公司、北京云科安信科技有限公司（Seraph 安全实验室）、山石网科通信技术股份有限公司、陕西省网络与信息安全测评中心、快页信息技术有限公司、内蒙古洞明科技有限公司、广州安亿信软件科技有限公司、广州百蕴启辰科技有限公司、广州易东信息安全技术有限公司、海南神州希望网路有限公司、天津偕行科技有限公司、北京机沃科技有限公司、浙江东安检测技术有限公司、北京水木羽林科技有限公司、思而听网络科技有限公司、苏州棱镜七彩信息科技有限公司、平安银河实验室、广西等保安全测评有限公司、联想集团及其他个人白帽子向 CNVD 提交了 10359 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 7773 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）	6067	6067
北京天融信网络安全技术有限公司	1773	100
奇安信网神（补天平	1133	1133

台）		
上海交大	573	573
北京神州绿盟科技有限公司	229	10
哈尔滨安天科技集团股份有限公司	229	0
新华三技术有限公司	215	0
北京数字观星科技有限公司	180	0
深信服科技股份有限公司	127	0
恒安嘉新（北京）科技股份公司	126	0
远江盛邦（北京）网络安全科技股份有限公司	71	71
天津市国瑞数码安全系统股份有限公司	59	0
北京启明星辰信息安全技术有限公司	50	6
南京联成科技发展股份有限公司	8	8
北京知道创宇信息技术有限公司	4	4
沈阳东软系统集成工程有限公司	2	2
西安四叶草信息技术有限公司	1	1
北京华顺信安科技有限公司	210	0
北京信联科汇科技有限公司	97	97
广东蓝爵网络安全技术股份有限公司	55	55
贵州多彩宝互联网服	37	37

务有限公司		
山东新潮信息技术有限公司	34	34
南京树安信息技术有限公司	33	33
重庆都会信息科技	28	28
安徽长泰科技有限公司	26	26
长春嘉诚信息技术股份有限公司	21	21
北京安帝科技有限公司	19	19
杭州海康威视数字技术股份有限公司	18	18
星云博创科技有限公司	16	16
杭州迪普科技股份有限公司	15	1
北京远禾科技有限公司	11	11
河南信安世纪科技有限公司	11	11
北京威努特技术有限公司	10	10
亚信科技（成都）有限公司	9	0
京东云安全	9	9
河南灵创电子科技有限公司	8	8
上海纽盾科技股份有限公司	8	8
山东云天安全技术有限公司	8	8
福建省海峡信息技术有限公司	7	7

博智安全科技股份有限公司	7	7
北京云科安信科技有限公司（Seraph 安全实验室）	6	6
山石网科通信技术股份有限公司	6	6
陕西省网络与信息安全测评中心	4	4
快页信息技术有限公司	4	4
内蒙古洞明科技有限公司	3	3
广州安亿信软件科技有限公司	2	2
广州百蕴启辰科技有限公司	2	2
广州易东信息安全技术有限公司	2	2
海南神州希望网路有限公司	2	2
天津偕行科技有限公司	2	2
北京机沃科技有限公司	1	1
浙江东安检测技术有限公司	1	1
北京水木羽林科技有限公司	1	1
思而听网络科技有限公司	1	1
苏州棱镜七彩信息科技有限公司	1	1
平安银河实验室	1	1
广西等保安全测评有	1	1

限公司		
联想集团	1	1
CNCERT 北京分中心	3	3
CNCERT 浙江分中心	1	1
CNCERT 贵州分中心	1	1
个人	1874	1874
报送总计	13464	10359

本周漏洞按类型和厂商统计

本周，CNVD 收录了 553 个漏洞。WEB 应用 239 个，应用程序 193 个，网络设备（交换机、路由器等网络端设备）68 个，智能设备（物联网终端设备）19 个，操作系统 18 个，安全产品 14 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	239
应用程序	193
网络设备（交换机、路由器等网络端设备）	68
智能设备（物联网终端设备）	19
操作系统	18
安全产品	14
数据库	2

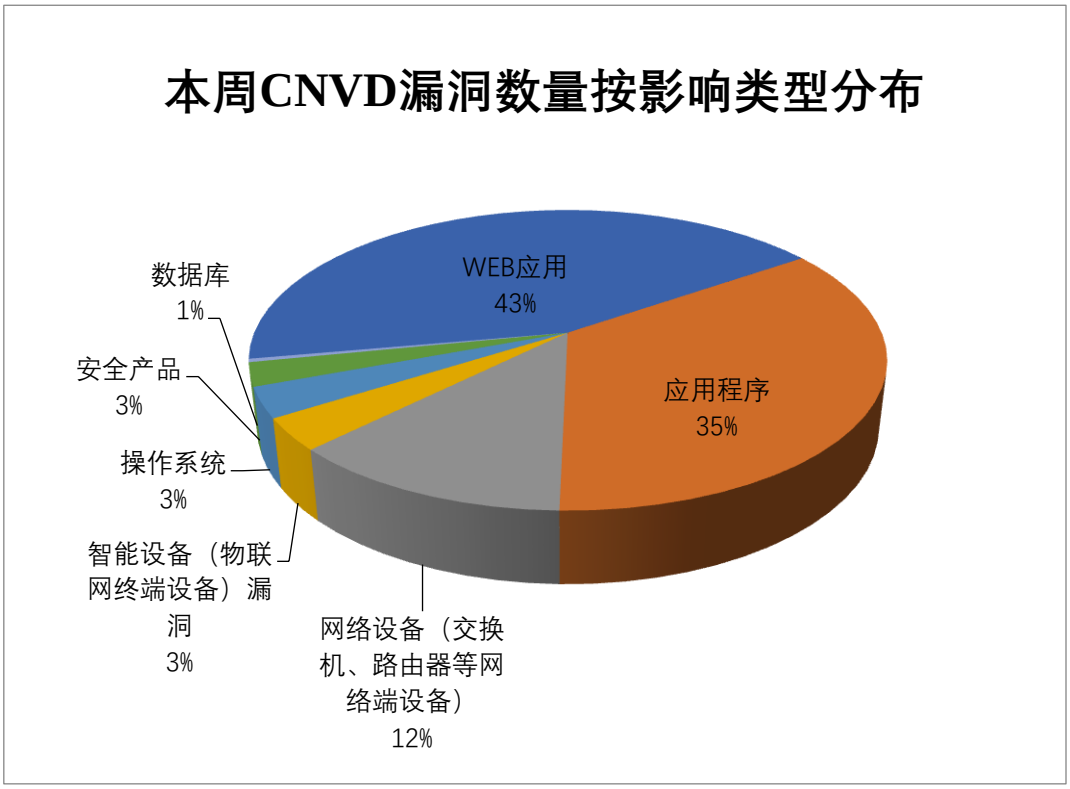

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Adobe、IBM、DELL 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	44	8%
2	IBM	32	6%
3	DELL	24	4%
4	Advantech	22	4%
5	淮南市银泰软件科技有限公司	21	4%
6	新华三技术有限公司	20	4%
7	湖南壹拾捌号网络技术有限公司	17	3%
8	Google	15	3%
9	WordPress	14	2%
10	其他	344	62%

本周行业漏洞收录情况

本周，CNVD 收录了 46 个电信行业漏洞，29 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，“D-Link DWR-932C E1 命令注入漏洞、Huawei Emui

和 Magic UI 资源管理错误漏洞”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/

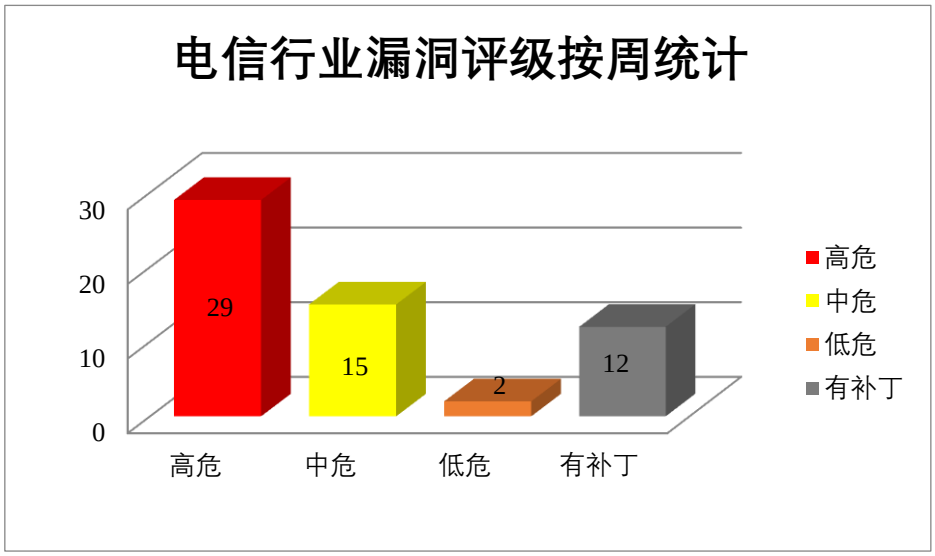

图 3 电信行业漏洞统计

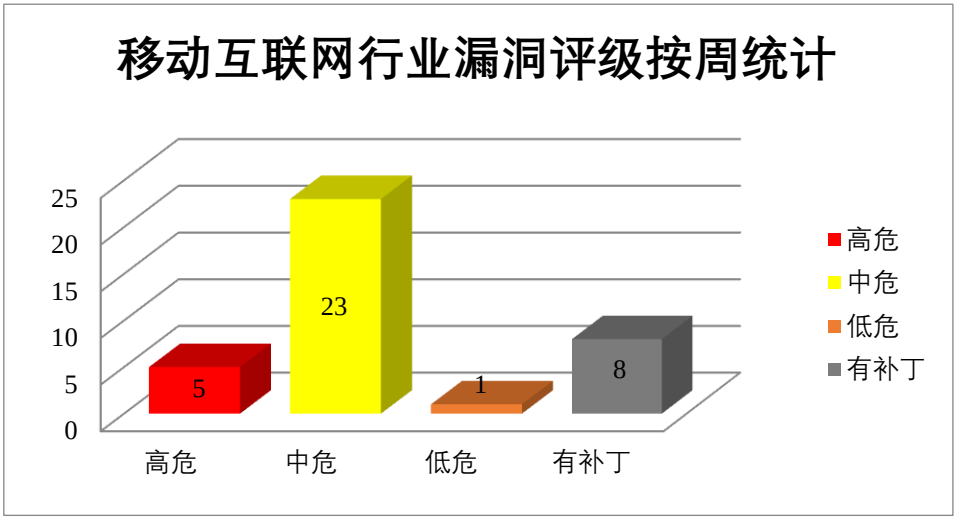

图 4 移动互联网行业漏洞统计

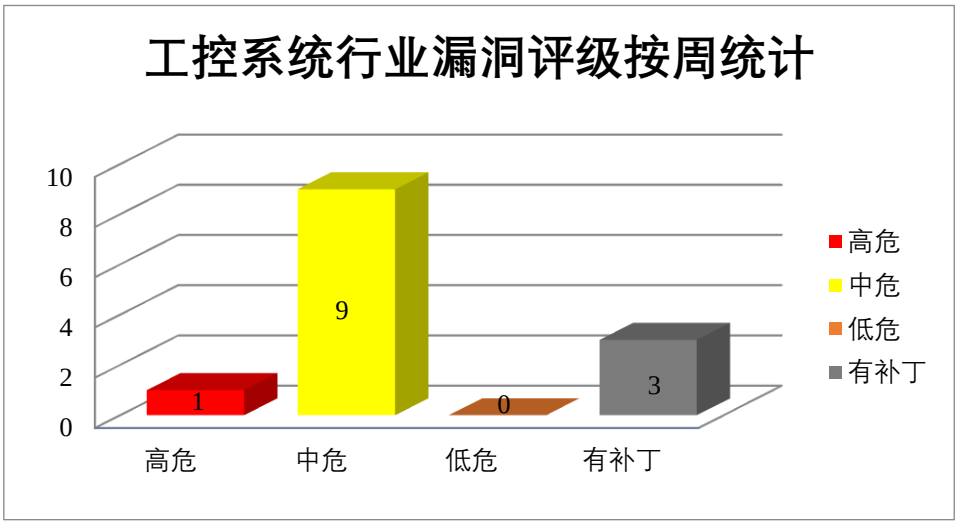

图 5 工控系统行业漏洞统计

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、DELL 产品安全漏洞

Dell Networking OS10 是美国戴尔（DELL）公司的一套基于 Linux 的网络交换机操作系统。Dell Networking X-Series 是美国戴尔（Dell）公司的一系列智能网管交换机。Dell EMC CloudLink 是一种灵活的数据加密和密钥管理解决方案，适用于公共、私有和混合云环境中的数据加密。Dell Bios 是美国戴尔（Dell）公司的一个计算机主板上小型内存芯片上的嵌入式软件。Dell OpenManage Enterprise 是美国 Dell 公司的一款用于 IT 基础架构管理的易于使用的一对多系统管理控制台。该软件支持一个控制台中经济高效地为 Dell EMC PowerEdge 服务器提供全面的生命周期管理。DELL EMC OpenManage Enterprise-Modular 是美国戴尔（DELL）公司的一个应用程序。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对受影响系统的访问并执行操作，通过伪造会话 ID 来劫持会话并访问网络服务器，获得受影响系统的管理员权限，在最终用户系统上执行任意文件等。

CNVD 收录的相关漏洞包括：Dell Networking OS10 身份验证绕过漏洞、Dell Networking X-Series 身份验证绕过漏洞、Dell Networking OS10 权限提升漏洞、Dell EMC CloudLink 任意文件创建漏洞、Dell BIOS 输入验证错误漏洞（CNVD-2021-92452、CNVD-2021-92544）、Dell OpenManage Enterprise 操作系统命令注入漏洞、DELL EMC OpenManage Enterprise-Modular 操作系统命令注入漏洞。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-2021-92436

https://www.cnvd.org.cn/flaw/show/CNVD-2021-92440

https://www.cnvd.org.cn/flaw/show/CNVD-2021-92437

https://www.cnvd.org.cn/flaw/show/CNVD-2021-92444

https://www.cnvd.org.cn/flaw/show/CNVD-2021-92452

https://www.cnvd.org.cn/flaw/show/CNVD-2021-92459

https://www.cnvd.org.cn/flaw/show/CNVD-2021-92461

https://www.cnvd.org.cn/flaw/show/CNVD-2021-92544

2、 Adobe 产品安全漏洞

Adobe XMP Toolkit SDK 是美国奥多比（Adobe）公司的一种标签技术，允许您将有关文件的数据（称为元数据）嵌入到文件本身中。Adobe Photoshop，简称“PS”，是由 Adobe 公司开发和发行的图像处理软件。Adobe Premiere Elements 是 Adobe 公司推出的一款视频编辑软件应用程序。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞执行任意代码。

CNVD 收录的相关漏洞包括：Adobe XMP Toolkit SDK 栈缓冲区溢出漏洞（CNVD-2021-91984、CNVD-2021-91983、CNVD-2021-91982、CNVD-2021-91985）、Adobe Photoshop 2021 缓冲区溢出漏洞、Adobe Photoshop 2021 内存缓冲区越界访问漏洞、Adobe Premiere Elements 内存缓冲区越界访问漏洞（CNVD-2021-91990、CNVD-2021-91994）。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-2021-91984

https://www.cnvd.org.cn/flaw/show/CNVD-2021-91983

https://www.cnvd.org.cn/flaw/show/CNVD-2021-91982

https://www.cnvd.org.cn/flaw/show/CNVD-2021-91985

https://www.cnvd.org.cn/flaw/show/CNVD-2021-91987

https://www.cnvd.org.cn/flaw/show/CNVD-2021-91988

https://www.cnvd.org.cn/flaw/show/CNVD-2021-91990

https://www.cnvd.org.cn/flaw/show/CNVD-2021-91994

3、 Advantech 产品安全漏洞

Advantech R-SeeNet 是中国台湾研华（Advantech）公司的一个工业监控软件。该软件基于 snmp 协议进行监控平台，并且适用于 Linux、Windows 平台。本周，上述产品被披露存在多个漏洞，攻击者可利用该漏洞通过发送精心设计的 HTTP 请求导致任意 PHP 代码执行，在数据库中执行任意 SQL 查询。

CNVD 收录的相关漏洞包括：Advantech R-SeeNet 文件包含漏洞、Advantech R-SeeNet SQL 注入漏洞（CNVD-2021-92433、CNVD-2021-92432、CNVD-2021-92435、CNVD-2021-92434、CNVD-2021-93820、CNVD-2021-93822、CNVD-2021-93821）。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-2021-92258
https://www.cnvd.org.cn/flaw/show/CNVD-2021-92433
https://www.cnvd.org.cn/flaw/show/CNVD-2021-92432
https://www.cnvd.org.cn/flaw/show/CNVD-2021-92435
https://www.cnvd.org.cn/flaw/show/CNVD-2021-92434
https://www.cnvd.org.cn/flaw/show/CNVD-2021-93820
https://www.cnvd.org.cn/flaw/show/CNVD-2021-93822
https://www.cnvd.org.cn/flaw/show/CNVD-2021-93821

4、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 SiteProtector System 是美国 IBM 公司的一个集中式管理系统。用于对网络、服务器和桌面端点安全代理以及小型网络或设备的统一管理和分析。IBM MQ（前身为 IBM WebSphere MQ）是一个强大、安全且可靠的消息传递中间件。IBM QRadar SIEM 是美国 IBM 公司的一套利用安全智能保护资产和信息远离高级威胁的解决方案。该方案提供对整个 IT 架构范围进行监督、生成详细的数据访问和用户活动报告等功能。IBM Business Automation Workflow 是一套工作流程自动化解决方案。该产品主要用于工作流程管理、合规性管理，并具有工作流程可见性和可扩展等特点。IBM System x servers 是美国国际商业机器公司（IBM）的一款服务器。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，经过身份验证的 SSH 或 Telnet 会话执行操作系统命令，导致拒绝服务等。

CNVD 收录的相关漏洞包括：IBM Planning Analytics 注入漏洞、IBM Tivoli Key Lifecycle Manager 拒绝服务漏洞、IBM SiteProtector Appliance 信息泄露漏洞、IBM MQ 拒绝服务漏洞（CNVD-2021-93631）、IBM QRadar SIEM 跨站脚本漏洞（CNVD-2021-94164）、IBM QRadar SIEM 信息泄露漏洞（CNVD-2021-94163）、IBM Business Automation Workflow 跨站脚本漏洞（CNVD-2021-94166）、IBM System x servers 操作系统命令注入漏洞。其中，“IBM Planning Analytics 注入漏洞、IBM System x servers 操作系统命令注入漏洞”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-2021-92467
https://www.cnvd.org.cn/flaw/show/CNVD-2021-92545
https://www.cnvd.org.cn/flaw/show/CNVD-2021-93383
https://www.cnvd.org.cn/flaw/show/CNVD-2021-93631

https://www.cnvd.org.cn/flaw/show/CNVD-2021-94164

https://www.cnvd.org.cn/flaw/show/CNVD-2021-94163

https://www.cnvd.org.cn/flaw/show/CNVD-2021-94166

https://www.cnvd.org.cn/flaw/show/CNVD-2021-94165

5、DOPSoft 栈缓冲区溢出漏洞

DOPSoft 是 Delta Electronics 公司推出的一款人机界面(HMI)编程软件。本周，DOPSoft 4.00.11 及更早版本存在栈缓冲区溢出漏洞，攻击者可通过特制项目文件利用该漏洞执行任意代码。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-2021-93912

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-2021-92462	baserCMS 操作系统命令注入漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://github.com/baserproject/basercms/security/advisories/GHSA-7rpc-9m88-cf9w
CNVD-2021-92466	Alfasado PowerCMS 操作系统命令注入漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：http://www.rtpro.yamaha.co.jp/RT/FAQ/Security/JVNVU91161784.html
CNVD-2021-92464	backstage 跨站脚本漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://github.com/backstage/backstage/security/advisories/GHSA-w7fj-336r-vw49
CNVD-2021-92540	Moodle 输入验证错误漏洞（CNVD-2021-92540）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://moodle.org/mod/forum/discuss.php?d=429095&parent=1726798
CNVD-2021-92825	ZTE MF971R 栈缓冲区溢出漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://support.zte.com.cn/support/news/LoopholeInfoDetail.aspx?newsId=1019764
CNVD-2021-92824	ZTE MF971R 栈缓冲区溢出漏洞（CNVD-2021-92824）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://support.zte.com.cn/support/ne

			ws/LoopholeInfoDetail.aspx?newsId=1019764
CNVD-2021-93382	Palo Alto Networks PAN-OS 操作系统命令注入漏洞（CNVD-2021-93382）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://security.paloaltonetworks.com/CVE-2021-3061
CNVD-2021-93381	Palo Alto Networks PAN-OS SCEP feature 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://security.paloaltonetworks.com/CVE-2021-3060
CNVD-2021-93840	Huawei AnyOffice 产品反序列化漏洞	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.huawei.com/en/psirt/security-advisories/huawei-sa-20210619-01-injection-en
CNVD-2021-93839	Huawei Emui 和 Magic UI 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，详情请关注厂商主页：https://consumer.huawei.com/en/support/bulletin/2021/5/

小结：本周，DELL 产品被披露存在多个漏洞，攻击者可利用该漏洞获取对受影响系统的访问并执行操作，通过伪造会话 ID 来劫持会话并访问网络服务器，获得受影响系统的管理员权限，在最终用户系统上执行任意文件等。此外，Adobe，Advantech，IBM 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精心设计的 HTTP 请求导致任意 PHP 代码执行，在数据库中执行任意 SQL 查询，获取敏感信息，经过身份验证的 SSH 或 Telnet 会话执行操作系统命令，导致拒绝服务，执行任意代码等。另外，DOPSoft 4.00.11 及更早版本被披露存在栈缓冲区溢出漏洞，攻击者可通过特制项目文件利用该漏洞执行任意代码。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、Phpjabbers Appointment Scheduler 跨站脚本漏洞

验证描述

Phpjabbers Appointment Scheduler 是塞尔维亚 Phpjabbers 公司的一个基于 Php 的用于规划时间，预定会议计划的预约时间表插件。

PHPJabbers Appointment Scheduler 2.3 存在跨站脚本漏洞，该漏洞源于在 index.php 管理登录页面(具有不同的请求参数)中，远程攻击者可利用该漏洞注入任意 web 脚本或 HTML。

验证信息

POC 链接：https://www.exploit-db.com/exploits/49281

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2021-94154

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. CISA 警告称 Zoho ManageEngine ServiceDesk 的关键漏洞已被利用

美国联邦调查局（FBI）和网络安全与基础设施安全局（CISA）警告说，Zoho 的 ManageEngine ServiceDesk Plus 产品中一个新修补的缺陷被积极利用。

参考链接：https://thehackernews.com/2021/12/cisa-warns-of-actively-exploited.html

2. 去中心化金融平台 BadgerDAO 遭黑客攻击，损失超过 1.2 亿美元

黑客从连接到去中心化金融平台 BadgerDAO 的多个加密货币钱包中窃取了价值 1.2 亿美元的各种代币。

参考链接：https://www.cnbeta.com/articles/tech/1210257.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