国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2021 年 12 月 06 日-2021 年 12 月 12 日 **2021 年第 49 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 658 个，其中高危漏洞 176 个、中危漏洞 430 个、低危漏洞 52 个。漏洞平均分值为 5.73。本周收录的漏洞中，涉及 0day 漏洞 387 个（占 59%），其中互联网上出现“WordPress Survey And Poll SQL 注入漏洞、Sourcecodester Alumni Management System 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原创漏洞总数 35692 个，与上周（10359 个）环比增加 245%。

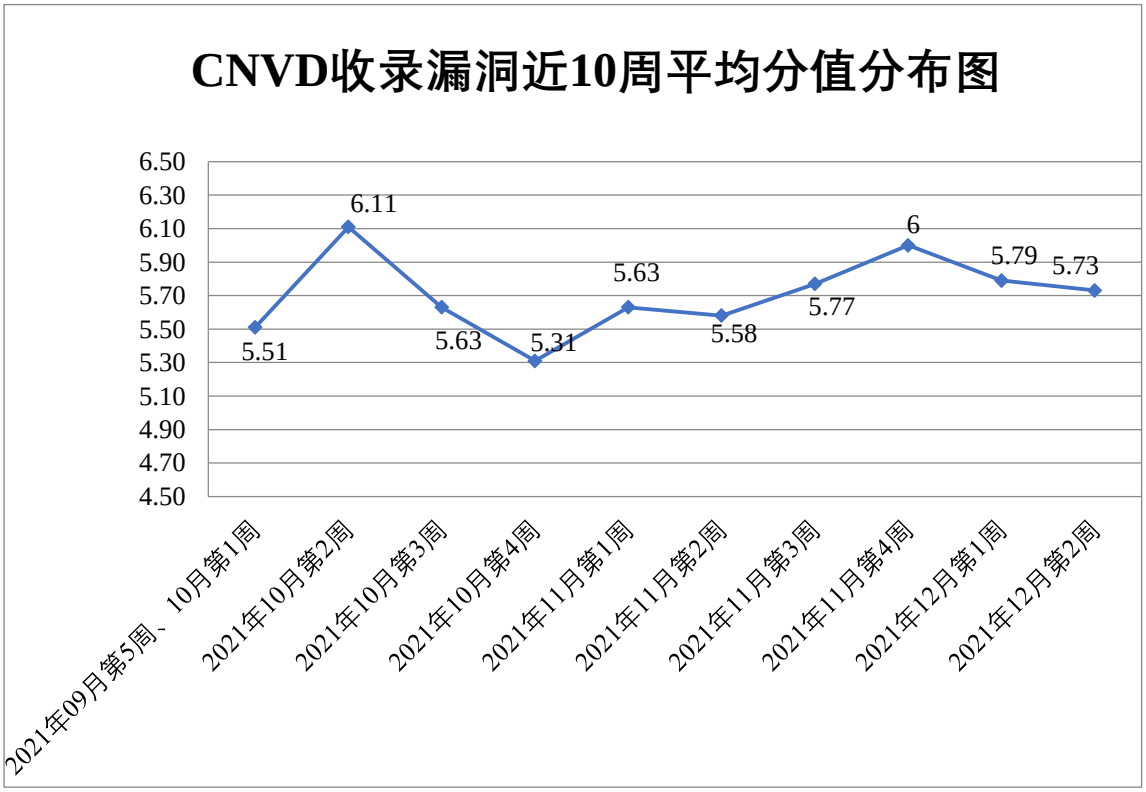

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 24 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 581 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 191 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 90 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、重庆聚合科技有限公司、中科博华信息科技有限公司、长沙市灵心康复器材有限公司、友讯电子设备（上海）有限公司、兄弟（中国）商业有限公司、新天科技股份有限公司、武汉捷讯信息技术有限公司、武汉烽火众智数字技术有限责任公司、网经科技（苏州）有限公司、天津神州浩天科技有限公司、苏州万户网络科技有限公司、苏州托普斯网络科技有限公司、泗洪雷速软件有限公司、四平市九州易通科技有限公司、四创科技有限公司、世邦通信股份有限公司、石家庄市征红网络科技有限公司、深圳市西迪特科技有限公司、深圳市微耕实业有限公司、深圳市必联电子有限公司、上海卓卓网络科技有限公司、上海亿速网络科技有限公司、上海蓝山办公软件有限公司、上海斐讯数据通信技术有限公司、上海泛微网络科技股份有限公司、上海贝锐信息科技股份有限公司、上海阿法迪智能数字科技股份有限公司、山西先启科技有限公司、山东潍微科技股份有限公司、山东金钟科技集团股份有限公司、厦门昕桐科技有限公司、厦门海为科技有限公司、三星（中国）投资有限公司、普联技术有限公司、欧姆龙（中国）有限公司、南京云网汇联软件技术有限公司、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、辽宁畅通数据通信有限公司、浪潮通用软件有限公司、金华市宁志网络科技有限公司、江苏金智教育信息股份有限公司、佳能（中国）有限公司、惠普贸易（上海）有限公司、湖南强智科技发展有限公司、湖南翱云网络科技有限公司、衡水金航计算机科技有限公司、杭州奕锐电子有限公司、杭州三汇信息工程有限公司、杭州合泰软件有限公司、杭州迪普科技股份有限公司、海南驰豹科技有限公司、海尔集团电子商务有限公司、贵州觅新科技有限公司、广州图创计算机软件开发有限公司、广州齐博网络科技有限公司、广州南方卫星导航仪器有限公司、广州合优网络科技有限公司、广东紫旭科技有限公司、广东环天电子技术发展有限公司、甘肃成兴信息科技有限公司、富士胶片（中国）投资有限公司、福建银达汇智信息科技股份有限公司、福建福昕软件开发股份有限公司、佛山市顺德区出格软件设计有限公司、成都索贝数码科技股份有限公司、成都思必得信息技术有限公司、常州文庭软件有限公司、北京中航讯科技股份有限公司、北京易讯思达科技开发有限公司、北京信安世纪科技股份有限公司、北京文网亿联科技有限公司、北京万户网络技术有限公司、北京天星组态软件有限公司、北京天生创想信息技术有限公司、北京魔方恒久软件有限公司、北京美特

软件技术有限公司、北京猎豹移动科技有限公司、北京慧图科技（集团）股份有限公司、北京爱奇艺科技有限公司、百度安全应急响应中心、爱普生（中国）有限公司、信呼、大米 CMS、中环 CMS、小说精品屋、物美智能、工作易人才招聘系统、XnSoft、Typecho、TwoThink、TOTOLINK、SEMCMS、Sapido Technology Inc、Opto22、Irfan Skiljan、Emerson、Dnsmasq、Belkin International,Inc、Bandisoft、Apache Software Foundation、Deciso B.V. 和 Adobe。

本周，CNVD 发布了《关于 Apache Log4j2 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/7116

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，厦门服云信息科技有限公司、北京天融信网络安全技术有限公司、新华三技术有限公司、哈尔滨安天科技集团股份有限公司、恒安嘉新（北京）科技股份公司等单位报送公开收集的漏洞数量较多。新疆海狼科技有限公司、北京华顺信安科技有限公司、北京信联科汇科技有限公司、河南信安世纪科技有限公司、河南灵创电子科技有限公司、广东蓝爵网络安全技术股份有限公司、山东新潮信息技术有限公司、南京树安信息技术有限公司、北京山石网科信息技术有限公司、快页信息技术有限公司、浙江木链物联网科技有限公司、京东云安全、北京安帝科技有限公司、重庆都会信息科技有限公司、上海纽盾科技股份有限公司、南京领行科技股份有限公司、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）、广州易东信息安全技术有限公司、福建省海峡信息技术有限公司、安徽长泰科技有限公司、平安银河实验室、浙江大华技术股份有限公司、星云博创科技有限公司、北京机沃科技有限公司、深圳市魔方安全科技有限公司、北京百度网讯科技有限公司、河南天祺信息安全技术有限公司、山东云天安全技术有限公司、思而听网络科技有限公司、百度 AIoT 安全团队、浙江大学控制科学与工程学院、内蒙古洞明科技有限公司、北京时代新威信息技术有限公司、四川博恩信息技术有限公司、北京君云天下科技有限公司、北京边界无限科技有限公司、杭州天谷信息科技有限公司及其他个人白帽子向 CNVD 提交了 35692 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 30259 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
奇安信网神（补天平台）	20043	20043
斗象科技（漏洞盒子）	8556	8556

上海交大	1660	1660
厦门服云信息科技有限公司	316	0
北京天融信网络安全技术有限公司	309	14
新华三技术有限公司	307	0
哈尔滨安天科技集团股份有限公司	242	0
恒安嘉新（北京）科技股份公司	121	0
深信服科技股份有限公司	116	0
北京神州绿盟科技有限公司	111	5
北京数字观星科技有限公司	95	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
北京启明星辰信息安全技术有限公司	53	1
杭州安恒信息技术股份有限公司	37	15
西安四叶草信息技术有限公司	16	16
远江盛邦（北京）网络安全科技股份有限公司	7	7
南京联成科技发展股份有限公司	6	6
阿里云计算有限公司	2	2
深圳市腾讯计算机系统有限公司（玄武实验室）	1	1

新疆海狼科技有限公司	254	254
北京华顺信安科技有限公司	185	4
北京信联科汇科技有限公司	115	115
河南信安世纪科技有限公司	76	76
河南灵创电子科技有限公司	75	75
广东蓝爵网络安全技术股份有限公司	55	55
山东新潮信息技术有限公司	55	55
南京树安信息技术有限公司	51	51
联想全球安全实验室	51	0
北京山石网科信息技术有限公司	49	49
快页信息技术有限公司	49	49
浙江木链物联网科技有限公司	39	39
京东云安全	32	32
北京安帝科技有限公司	24	24
重庆都会信息科技有限公司	19	19
杭州迪普科技股份有限公司	13	0
亚信科技（成都）有限公司	12	0
上海纽盾科技股份有限公司	10	10
南京领行科技股份有	9	9

限公司		
博智安全科技股份有限公司	8	8
北京云科安信科技有限公司（Seraph 安全实验室）	7	7
广州易东信息安全技术有限公司	6	6
福建省海峡信息技术有限公司	5	5
安徽长泰科技有限公司	4	4
平安银河实验室	4	4
浙江大华技术股份有限公司	4	4
星云博创科技有限公司	3	3
北京机沃科技有限公司	3	3
深圳市魔方安全科技有限公司	3	3
北京百度网讯科技有限公司	3	3
河南天祺信息安全技术有限公司	2	2
山东云天安全技术有限公司	2	2
思而听网络科技有限公司	2	2
百度 AIoT 安全团队	2	2
浙江大学控制科学与工程学院	1	1
内蒙古洞明科技有限公司	1	1
北京时代新威信息技	1	1

术有限公司		
四川博恩信息技术有限公司	1	1
北京君云天下科技有限公司	1	1
北京边界无限科技有限公司	1	1
杭州天谷信息科技有限公司	1	1
CNCERT 贵州分中心	4	4
个人	4381	4381
报送总计	37680	35692

本周漏洞按类型和厂商统计

本周，CNVD 收录了 658 个漏洞。WEB 应用 345 个，应用程序 192 个，网络设备（交换机、路由器等网络端设备）71 个，智能设备（物联网终端设备）23 个，操作系统 17 个， 安全产品 7 个，数据库 3 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	345
应用程序	192
网络设备（交换机、路由器等网络端设备）	71
智能设备（物联网终端设备）	23
操作系统	17
安全产品	7
数据库	3

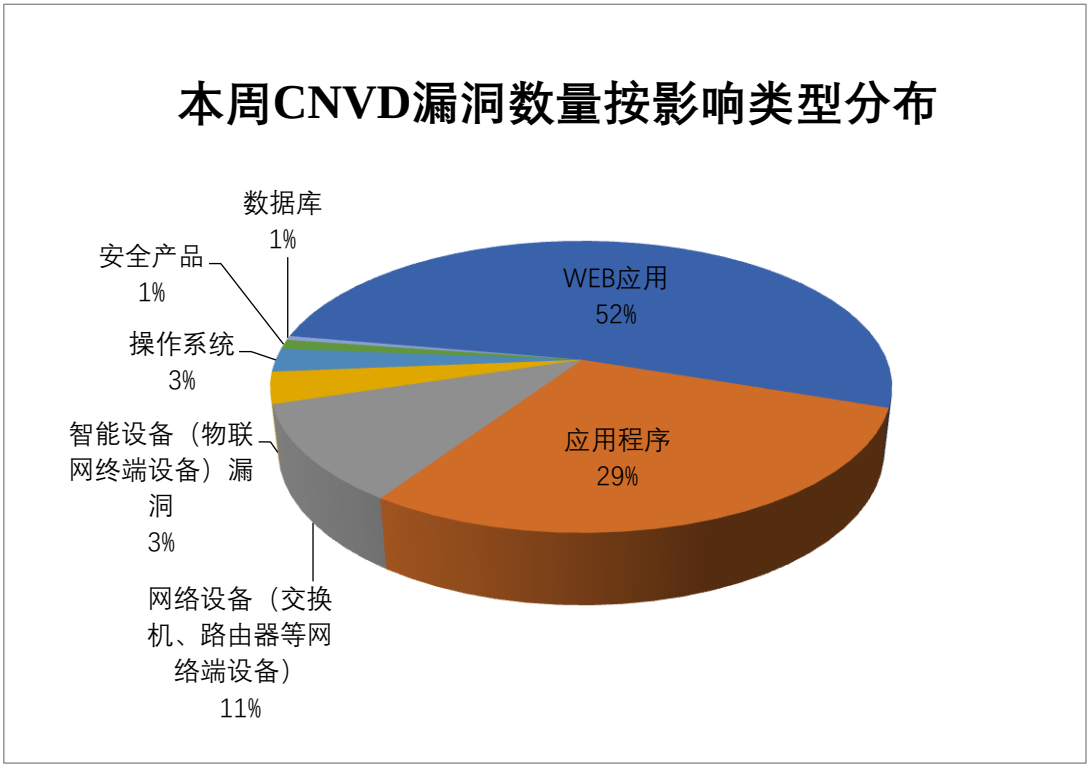

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及石家庄市征红网络科技有限公司、淄博闪灵网络科技有限公司、D-Link 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	石家庄市征红网络科技有限公司	42	6%
2	淄博闪灵网络科技有限公司	25	4%
3	D-Link	25	4%
4	SourceCodester	23	4%
5	无忧网络	17	3%
6	Dell	16	2%
7	淮南市银泰软件科技有限公司	15	2%
8	IBM	15	2%
9	Unitrends	13	2%
10	其他	467	71%

本周行业漏洞收录情况

本周，CNVD 收录了 58 个电信行业漏洞，7 个移动互联网行业漏洞，6 个工控行业漏洞（如下图所示）。其中，“D-Link DIR-615 缓冲区溢出漏洞、D-LINK DIR-3040

信息泄露漏洞（CNVD-2021-94832）”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/

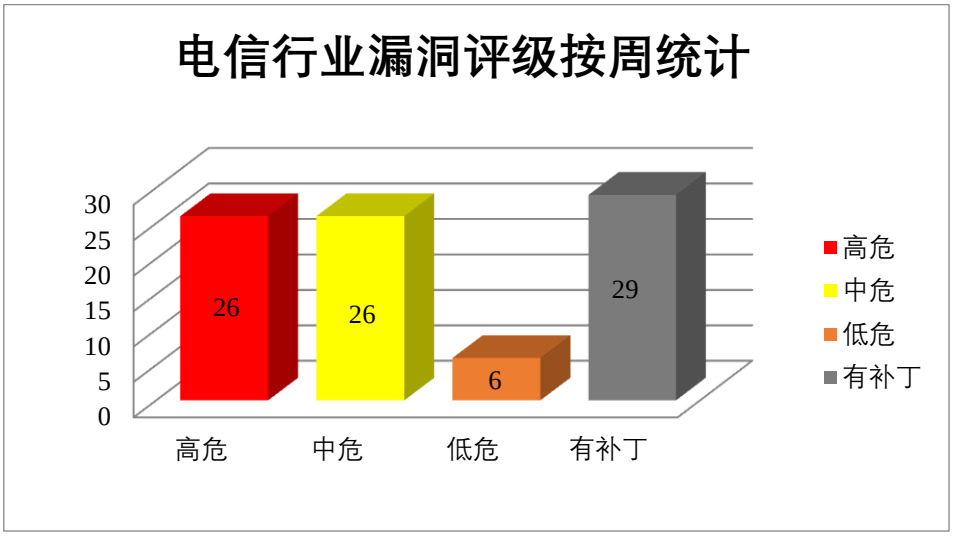

图 3 电信行业漏洞统计

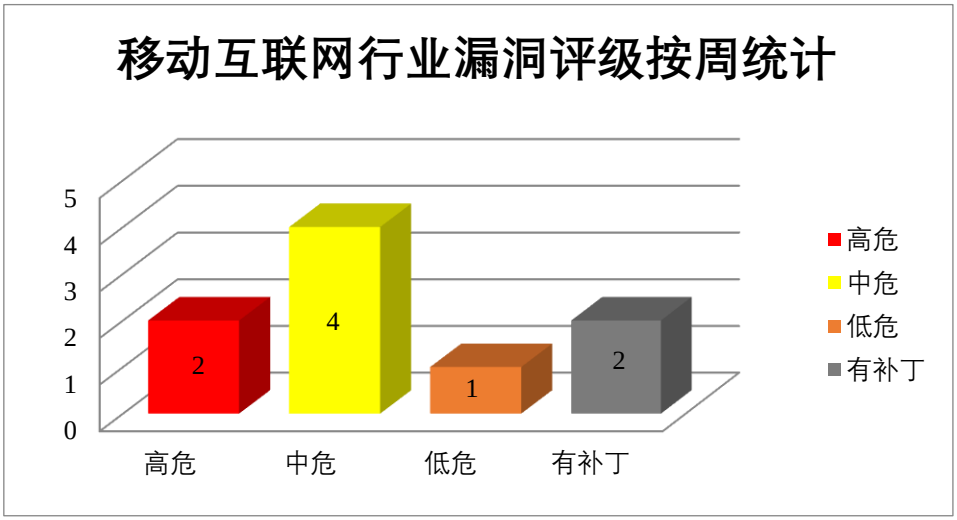

图 4 移动互联网行业漏洞统计

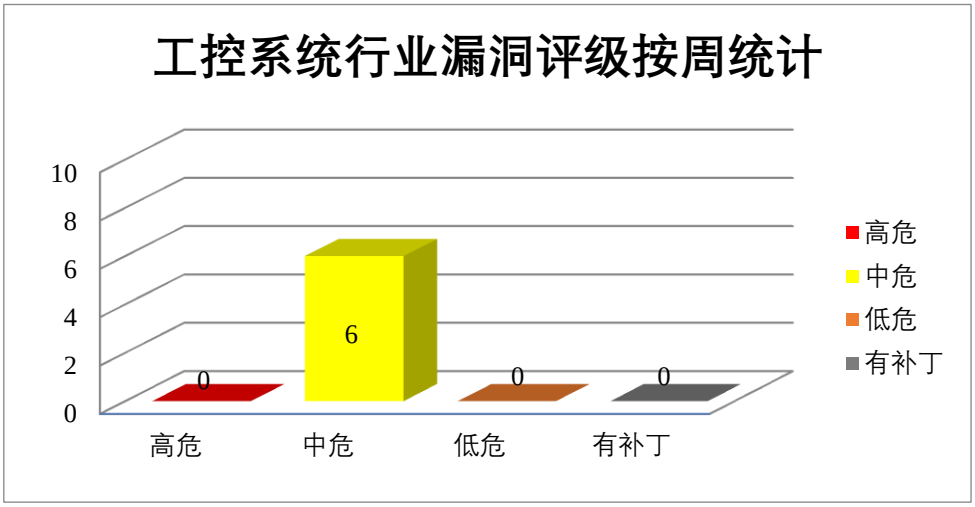

图 5 工控系统行业漏洞统计

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 Reader（也被称为 Acrobat Reader）是 Adobe 公司开发的一款 PDF 文件阅读软件。Adobe Acrobat 是由 Adobe 公司开发的一款 PDF 编辑软件。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞读取任意文件系统，执行任意代码等。

CNVD 收录的相关漏洞包括：Adobe Acrobat/Reader 释放后重用漏洞（CNVD-2021-94911、CNVD-2021-94912、CNVD-2021-94913、CNVD-2021-94914）、Adobe Acrobat/Reader 栈缓冲区溢出漏洞（CNVD-2021-94917、CNVD-2021-94916）、Adobe Acrobat/Reader 越界写入漏洞（CNVD-2021-94918）、Adobe Acrobat/Reader 越界读取漏洞（CNVD-2021-94939）。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-2021-94911

https://www.cnvd.org.cn/flaw/show/CNVD-2021-94912

https://www.cnvd.org.cn/flaw/show/CNVD-2021-94913

https://www.cnvd.org.cn/flaw/show/CNVD-2021-94914

https://www.cnvd.org.cn/flaw/show/CNVD-2021-94917

https://www.cnvd.org.cn/flaw/show/CNVD-2021-94916

https://www.cnvd.org.cn/flaw/show/CNVD-2021-94918

https://www.cnvd.org.cn/flaw/show/CNVD-2021-94939

2、 D-Link 产品安全漏洞

D-Link DIR-809 是中国友讯（D-Link）公司的一款双频路由器。D-Link DIR-605L

是 D-link 公司推出的第一款云路由器，传输速度为 300Mpbs。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用户名和密码，导致拒绝服务或执行任意代码等。

CNVD 收录的相关漏洞包括：D-Link DIR-809 formStaticDHCP 缓冲区溢出漏洞、D-Link DIR-809 formSetPortTr 缓冲区溢出漏洞（CNVD-2021-94717）、D-Link DIR-809 formVirtualApp 缓冲区溢出漏洞、D-Link DIR-809 formVirtualServ 缓冲区溢出漏洞（CNVD-2021-94719）、D-Link DIR-809 formSetPortTr 缓冲区溢出漏洞、D-Link DIR-809 formWlanSetup 缓冲区溢出漏洞、D-Link DIR-809 formAdvFirewall 缓冲区溢出漏洞、D-Link DIR-605L 信息泄露漏洞。其中，除“D-Link DIR-605L 信息泄露漏洞”外，其余漏洞综合评级为“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-2021-94716
https://www.cnvd.org.cn/flaw/show/CNVD-2021-94717
https://www.cnvd.org.cn/flaw/show/CNVD-2021-94718
https://www.cnvd.org.cn/flaw/show/CNVD-2021-94719
https://www.cnvd.org.cn/flaw/show/CNVD-2021-94721
https://www.cnvd.org.cn/flaw/show/CNVD-2021-94723
https://www.cnvd.org.cn/flaw/show/CNVD-2021-94722
https://www.cnvd.org.cn/flaw/show/CNVD-2021-94835

3、Dell 产品安全漏洞

Dell EMC iDRAC9 是美国戴尔（DELL）公司的一套包含硬件和软件的系统管理解决方案。该方案为 Dell PowerEdge 系统提供远程管理、崩溃系统恢复和电源控制等功能。Dell EMC PowerFlex 是美国戴尔（DELL）公司的一个应用软件。提供极高的灵活性和可扩展性，以及企业级性能和弹性，同时简化基础设施的管理和操作。Dell Open Manage Enterprise 是美国戴尔（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 PowerEdge Server BIOS 是美国戴尔（DELL）公司的一款系统更新驱动程序。Dell Emc Streaming Data Platform 是美国戴尔（Dell）公司的一个用于实时摄取、存储和分析连续流数据的平台。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞欺骗受害者用户点击恶意制作的链接，将用户重定向到任意的链接地址，执行非法 SQL 命令，导致客户端代码执行等。

CNVD 收录的相关漏洞包括：Dell EMC iDRAC9 跨站脚本漏洞（CNVD-2021-94891、CNVD-2021-94895、CNVD-2021-94894）、Dell EMC iDRAC9 输入验证错误漏洞（CNVD-2021-94890）、Dell powerflex presentation server 数据伪造问题漏洞、Dell OpenManage Enterprise 操作系统命令注入漏洞、Dell PowerEdge 缓冲区溢出漏洞、Dell EMC Streaming Data Platform SQL 注入漏洞。其中，“Dell PowerEdge 缓冲区溢出漏

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-2021-94891

https://www.cnvd.org.cn/flaw/show/CNVD-2021-94890

https://www.cnvd.org.cn/flaw/show/CNVD-2021-94896

https://www.cnvd.org.cn/flaw/show/CNVD-2021-94895

https://www.cnvd.org.cn/flaw/show/CNVD-2021-94894

https://www.cnvd.org.cn/flaw/show/CNVD-2021-94898

https://www.cnvd.org.cn/flaw/show/CNVD-2021-94897

https://www.cnvd.org.cn/flaw/show/CNVD-2021-95602

4、ZOHO 产品安全漏洞

ZOHO ManageEngine SupportCenter Plus 是 ZOHO 公司的一种基于 Web 的客户支持软件。ZOHO ManageEngine M365 Manager Plus 是 ZOHO 公司的一个广泛 Microsoft 365 工具。ZOHO ManageEngine ADManager Plus 是美国 Zoho 公司的一个 Active Directory (AD) 管理和报告解决方案。ZOHO ManageEngine Log360 是美国卓豪（ZOHO）公司的一个集成的日志管理和 Active Directory 审计和警报解决方案。ZOHO ManageEngine Network Configuration Manager 是美国 ZOHO 公司的一种多供应商网络变更、配置和合规性管理 (Nccm) 解决方案。ZOHO ManageEngine ServiceDesk Plus（SDP）是美国卓豪（ZOHO）公司的一套基于 ITIL 架构的 IT 服务管理软件。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞通过 SSO 接管帐户，获取敏感数据，远程执行代码等。

CNVD 收录的相关漏洞包括：ZOHO ManageEngine SupportCenter Plus 跨站脚本漏洞（CNVD-2021-94825、CNVD-2021-94824）、ZOHO ManageEngine M365 Manager Plus 文件上传漏洞、ZOHO ManageEngine ADManager Plus 授权问题漏洞、ZOHO ManageEngine Log360 访问控制错误漏洞、ZOHO ManageEngine Network Configuration Manager 命令注入漏洞、ZOHO ManageEngine SupportCenter Plus 服务器端请求伪造漏洞、ZOHO ManageEngine ServiceDesk Plus 远程代码执行漏洞。其中，“ZOHO ManageEngine M365 Manager Plus 文件上传漏洞、ZOHO ManageEngine ADManager Plus 授权问题漏洞、ZOHO ManageEngine Log360 访问控制错误漏洞、ZOHO ManageEngine Network Configuration Manager 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-2021-94825

https://www.cnvd.org.cn/flaw/show/CNVD-2021-94824

https://www.cnvd.org.cn/flaw/show/CNVD-2021-94823

https://www.cnvd.org.cn/flaw/show/CNVD-2021-94829

https://www.cnvd.org.cn/flaw/show/CNVD-2021-94828

https://www.cnvd.org.cn/flaw/show/CNVD-2021-94827

https://www.cnvd.org.cn/flaw/show/CNVD-2021-94826

https://www.cnvd.org.cn/flaw/show/CNVD-2021-94846

5、Philips Healthcare Tasy Electronic Medical Record (EMR) SQL 注入漏洞

Philips Healthcare Tasy Electronic Medical Record (EMR)是一个全面的医疗信息学解决方案，涉及医疗环境的所有领域，将医疗保健连续体中临床和非临床领域的点连接起来。本周，Philips Healthcare Tasy Electronic Medical Record (EMR)被披露存在 SQL 注入漏洞。攻击者可通过 CorCad_F2/executaConsultaEspecifico IE_CORPO_ASSIST 或 CD_USUARIO_CONVENIO 参数利用该漏洞进行 SQL 注入攻击。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-2021-94943

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-2021-94830	D-Link DIR-X6060 和 D-Link DIR-X1560 拒绝服务漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10243
CNVD-2021-94904	Apache Storm 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://lists.apache.org/thread.html/r5fe881f6ca883908b7a0f005d35115af49f43beea7a8b0915e377859%40%3Cuser.storm.apache.org%3E
CNVD-2021-94903	Linux kernel 释放后重用漏洞（CNVD-2021-94903）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=a3727a8bac0a9e77c70820655fd8715523ba3db7
CNVD-2021-94925	Centreon OS 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://github.com/centreon/ce

			ntreon/pull/8467#event-3163627607
CNVD-2021-94955	HMI3 Control Panel 信任管理问题漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://us-cert.cisa.gov/ics/advisories/icsma-21-215-01
CNVD-2021-94962	Microsoft Azure 权限许可和访问控制问题漏洞（CNVD-2021-94962）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-42303
CNVD-2021-94964	Monstra 远程代码执行漏洞（CNVD-2021-94964）	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/monstra-cms/monstra/issues/470
CNVD-2021-95249	ecshop SQL 注入漏洞（CNVD-2021-95249）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/shopex/ecshop/issues/4
CNVD-2021-95252	LibreDWG 缓冲区溢出漏洞（CNVD-2021-95252）	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/LibreDWG/libredwg/issues/325
CNVD-2021-94836	D-Link DIR-615 缓冲区溢出漏洞	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://www.dlink.com/en/security-bulletin/

小结：本周，Adobe 产品被披露存在多个漏洞，攻击者可利用漏洞读取任意文件系统，执行任意代码等。此外，D-Link、Dell、ZOHO 等多款产品被披露存在多个漏洞，攻击者可利用漏洞通过 SSO 接管帐户，获取敏感数据，执行非法 SQL 命令，远程执行代码等。另外，Philips Healthcare Tasy Electronic Medical Record (EMR) 被披露存在 SQL 注入漏洞。攻击者可通过 CorCad_F2/executaConsultaEspecifico IE_CORPO_ASSIST 或 CD_USUARIO_CONVENIO 参数利用该漏洞进行 SQL 注入攻击。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、WordPress Survey And Poll SQL 注入漏洞

验证描述

WordPress 是 Wordpress 基金会的一套使用 PHP 语言开发的博客平台。WordPress Survey and Poll 是网站上游客直接反馈的解决方案。

WordPress Survey And Poll SQL 注入漏洞，攻击者可利用漏洞获取数据库敏感信息。

验证信息

POC 链接：https://packetstormsecurity.com/files/164060/WordPress-Survey-And-Poll-1.5.7.3-SQL-Injection.html

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2021-95636

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. 9 款 WiFi 路由器 226 个漏洞影响数百万设备

IoT Inspector 和 CHIP 的安全研究人员合作对 Asus、AVM、D-Link、Netgear、Edimax、TP-Link、Synology 和 Linksys 等生产的 9 款主流的 WiFi 路由器进行了安全性分析，在其中发现了 226 个安全漏洞。其中 TP-Link Archer AX6000 路由器被披露安全漏洞最多，有 32 个，其次是 Synology RT-2600ac 路由器，有 30 个安全漏洞。

参考链接：https://www.4hou.com/posts/O6qN

2. Moobot 僵尸网络正利用海康威视产品漏洞传播

据 SecurityAffairs 消息，Moobot 僵尸网络正在利用海康威视产品的漏洞进行快速传播。这是海康威视网络摄像机/NVR 固件中，一个未经身份验证的远程代码执行（RCE）漏洞，编号为 CVE-2021-36260。

参考链接：https://www.freebuf.com/news/308208.html

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