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 27 日-2021 年 10 月 10 日 **2021 年第 39、40 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 677 个，其中高危漏洞 161 个、中危漏洞 446 个、低危漏洞 70 个。漏洞平均分值为 5.51。本周收录的漏洞中，涉及 0day 漏洞 600 个（占 89%），其中互联网上出现“MetInfo SQL 注入漏洞（CNVD-2021-74293）、Deskpro 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 9212 个，与上周（4843 个）环比增加 90%。

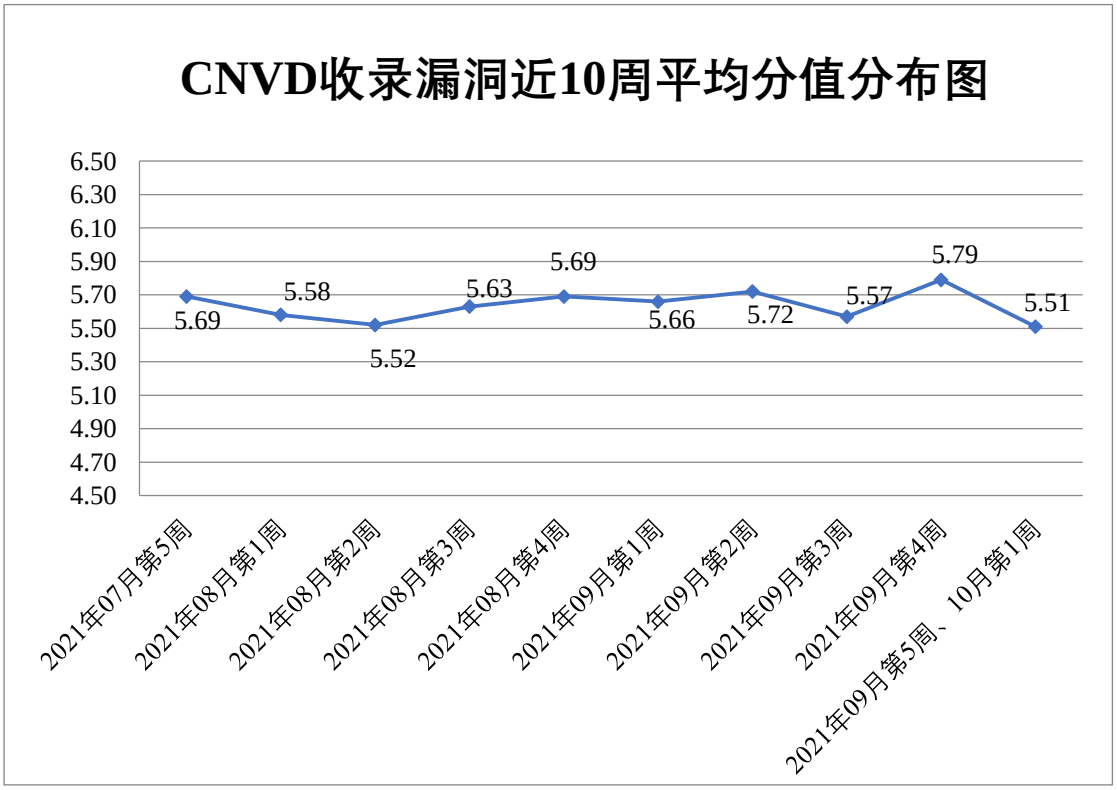

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 27 起，向基础电信企业通报漏洞事件 41 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 461 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 50 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 64 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、珠海金山办公软件有限公司、中铁合肥建筑市政工程设计研究院有限公司、中国大唐集团有限公司、浙江齐治科技股份有限公司、友讯电子设备（上海）有限公司、兄弟（中国）商业有限公司、西安兄弟信息科技有限公司、西安交大捷普网络科技有限公司、万商云集（成都）科技股份有限公司、太原迅易科技有限公司、松下电器（中国）有限公司、思科系统（中国）网络技术有限公司、思爱普（中国）有限公司、世邦通信股份有限公司、神州数码控股有限公司、深圳市乙辰科技股份有限公司、深圳市迅雷网络技术有限公司、深圳市尼高企业形象设计有限公司、深圳市锟铻科技有限公司、深圳市警安智能设备有限公司、深圳市捷视飞通科技股份有限公司、深圳市吉祥腾达科技有限公司、上海肯特仪表股份有限公司、上海凯京信达科技集团有限公司、上海建文软件科技有限公司、上海华测导航技术股份有限公司、上海复翼软件开发有限公司、熵基科技股份有限公司、汕头市东博网络科技有限公司、山东金钟科技集团股份有限公司、厦门市灵鹿谷科技有限公司、三星（中国）投资有限公司、全讯汇聚网络科技（北京）有限公司、南京怀宇科技有限公司、南京鸿名物联科技有限公司、南昌蓝智科技有限公司、六安校无忧信息科技有限公司、联奕科技股份有限公司、朗坤智慧科技股份有限公司、廊坊市极致网络科技有限公司、金蝶软件（中国）有限公司、佳能（中国）有限公司、湖南三通慧联科技有限公司、湖南建研信息技术股份有限公司、杭州帷拓科技有限公司、杭州海康威视数字技术股份有限公司、广州网易计算机系统有限公司、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、广州科密股份有限公司、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、飞天诚信科技股份有限公司、东北师大理想软件股份有限公司、成都星锐蓝海网络科技有限公司、北京亚控科技发展有限公司、北京星网锐捷网络技术有限公司、北京新网数码信息技术有限公司、北京网康科技有限公司、北京万户网络技术有限公司、北京青云科技股份有限公司、北京普艾斯科技有限公司、北京派网软件有限公司、北京南琼电子有限责任公司、北京国炬信息技术有限公司、北京棣南新宇科技有限公司、北京得特创新科技有限公司、北京博习园教育科技有限公司、北京佰才邦技术股份有限公司、北方互动科技（北京）有限公司、北大方正集团有限公司、中央电视台、腾讯安全应急响应中心、苹果 CMS、若依、ZZCMS、XnSoft、unicms、

The Apache Software Foundation、taoCMS、Rancher、PhpaaCMS、Lexmark、JreCms、Irfan Skiljan、gxcms、Eclipse 和 ACTi。

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、新华三技术有限公司、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、北京奇虎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、北京山石网科信息技术有限公司、河南灵创电子科技有限公司、联想集团、南京众智维信息科技有限公司、新疆海狼科技有限公司、亚信科技（成都）有限公司、河南信安世纪科技有限公司、广东蓝爵网络安全技术股份有限公司、京东云安全、安徽长泰科技有限公司、江苏快页信息技术有限公司、上海纽盾科技股份有限公司、北京信联科汇科技有限公司、浙江木链物联网科技有限公司、北京安帝科技有限公司、北京网御星云信息技术有限公司、江西省掌控者信息安全技术有限公司、北京大学、北京惠而特科技有限公司、星云博创科技有限公司、北京云科安信科技有限公司（Seraph 安全实验室）、泰山信息科技有限公司、山东新潮信息技术有限公司、北京天地和兴科技有限公司、北京远禾科技有限公司、山东泽鹿安全技术有限公司、内蒙古洞明科技有限公司、中移（杭州）信息技术有限公司、北京云弈科技有限公司、长春嘉诚信息技术股份有限公司、内蒙古云科数据服务股份有限公司、福建省海峡信息技术有限公司、云南南天电子信息产业股份有限公司、广州安亿信软件科技有限公司、中通服咨询设计研究院有限公司、思而听网络科技有限公司、杭州海康威视数字技术股份有限公司、重庆都会信息科技有限公司、南京树安信息技术有限公司、北京水木羽林科技有限公司、银保信科技(北京)有限公司、南京领行科技股份有限公司、腾讯公司、深圳市魔方安全科技有限公司、平安银河实验室及其他个人白帽子向 CNVD 提交了 9212 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 6021 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）	4413	4413
北京天融信网络安全技术有限公司	996	10
上海交大	918	918
奇安信网神（补天平台）	690	690
新华三技术有限公司	302	0

北京神州绿盟科技有限公司	288	19
哈尔滨安天科技集团股份有限公司	276	0
北京奇虎科技有限公司	228	0
深信服科技股份有限公司	197	0
北京启明星辰信息安全技术有限公司	153	96
恒安嘉新（北京）科技股份公司	153	0
北京数字观星科技有限公司	139	0
天津市国瑞数码安全系统股份有限公司	115	0
华为技术有限公司	95	0
远江盛邦（北京）网络安全科技股份有限公司	47	47
南京联成科技发展股份有限公司	23	23
浙江大华技术股份有限公司	16	16
西安四叶草信息技术有限公司	6	6
北京知道创宇信息技术有限公司	3	0
北京安信天行科技有限公司	2	2
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	371	371
北京山石网科信息技	196	196

术有限公司		
河南灵创电子科技有限公司	166	166
联想集团	151	0
南京众智维信息科技有限公司	69	69
新疆海狼科技有限公司	65	65
亚信科技（成都）有限公司	61	14
河南信安世纪科技有限公司	60	60
广东蓝爵网络安全技术股份有限公司	59	59
京东云安全	57	57
安徽长泰科技有限公司	57	57
江苏快页信息技术有限公司	47	47
上海纽盾科技股份有限公司	29	29
北京信联科汇科技有限公司	28	28
浙江木链物联网科技有限公司	27	27
北京华顺信安科技有限公司	25	0
北京安帝科技有限公司	24	24
北京网御星云信息技术有限公司	20	20
江西省掌控者信息安全技术有限公司	19	19
北京大学	17	17
北京惠而特科技有限	16	16

公司		
杭州迪普科技股份有限公司	13	0
星云博创科技有限公司	12	12
北京云科安信科技有限公司（Seraph 安全实验室）	7	7
泰山信息科技有限公司	7	7
山东新潮信息技术有限公司	6	6
北京天地和兴科技有限公司	6	6
北京远禾科技有限公司	5	5
山东泽鹿安全技术有限公司	4	4
内蒙古洞明科技有限公司	4	4
中移（杭州）信息技术有限公司	3	3
北京云弈科技有限公司	3	3
长春嘉诚信息技术股份有限公司	3	3
内蒙古云科数据服务股份有限公司	3	3
福建省海峡信息技术有限公司	3	3
云南南天电子信息产业股份有限公司	3	3
广州安亿信软件科技有限公司	3	3
中通服咨询设计研究	2	2

院有限公司		
思而听网络科技有限公司	2	2
杭州海康威视数字技术股份有限公司	2	2
重庆都会信息科技有限公司	2	2
南京树安信息技术有限公司	2	2
北京水木羽林科技有限公司	1	1
银保信科技(北京)有限公司	1	1
南京领行科技股份有限公司	1	1
腾讯公司	1	1
深圳市魔方安全科技有限公司	1	1
平安银河实验室	1	1
CNCERT 青海分中心	6	6
CNCERT 山西分中心	4	4
CNCERT 吉林分中心	2	2
CNCERT 云南分中心	1	1
个人	1532	1529
报送总计	12271	9212

本周漏洞按类型和厂商统计

本周，CNVD 收录了 677 个漏洞。WEB 应用 279 个，应用程序 162 个，网络设备（交换机、路由器等网络端设备）142 个，智能设备（物联网终端设备）59 个，数据库 15 个，操作系统 11 个，安全产品 9 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	279
应用程序	162

网络设备（交换机、路由器等网络端设备）	142
智能设备（物联网终端设备）	59
数据库	15
操作系统	11
安全产品	9

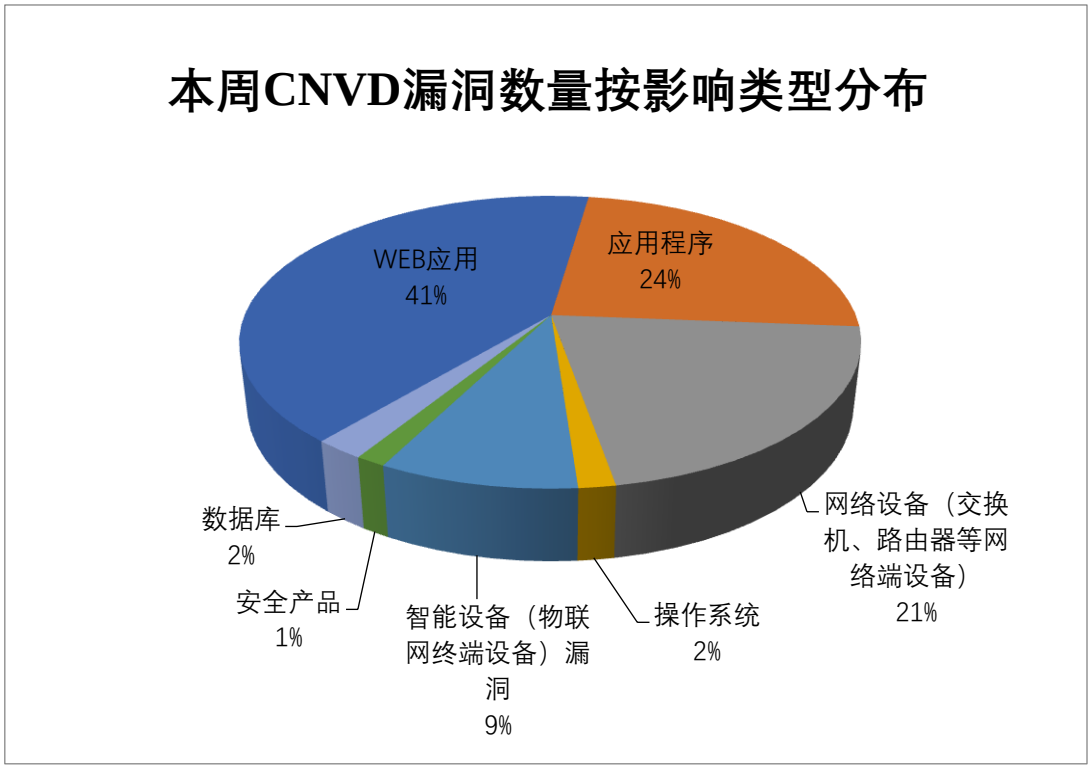

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 D-Link、Lexmark International Inc、Adobe 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	D-Link	74	11%
2	Lexmark International Inc	29	4%
3	Adobe	17	3%
4	JEESNS	17	2%
5	Microsoft	13	2%
6	EmpireCMS	12	2%
7	lmxcms	11	1%
8	DELL	10	1%
9	VMWare	10	1%
10	其他	484	73%

本周行业漏洞收录情况

本周，CNVD 收录了 114 个电信行业漏洞，21 个移动互联网行业漏洞，11 个工控行业漏洞（如下图所示）。

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/

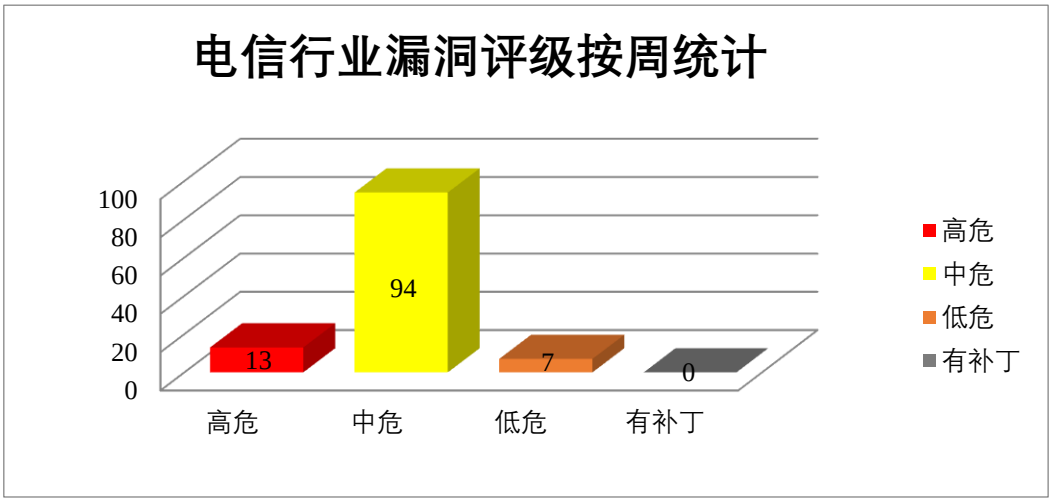

图 3 电信行业漏洞统计

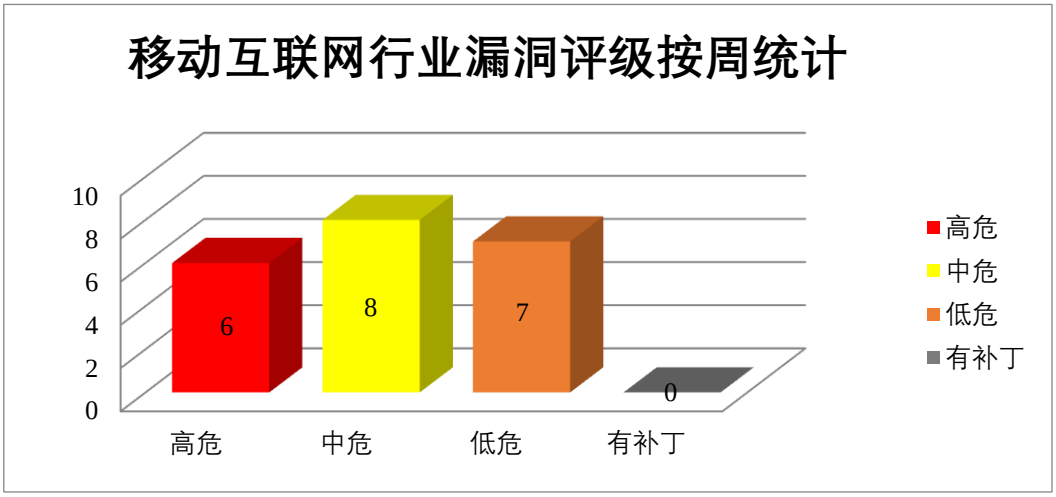

图 4 移动互联网行业漏洞统计

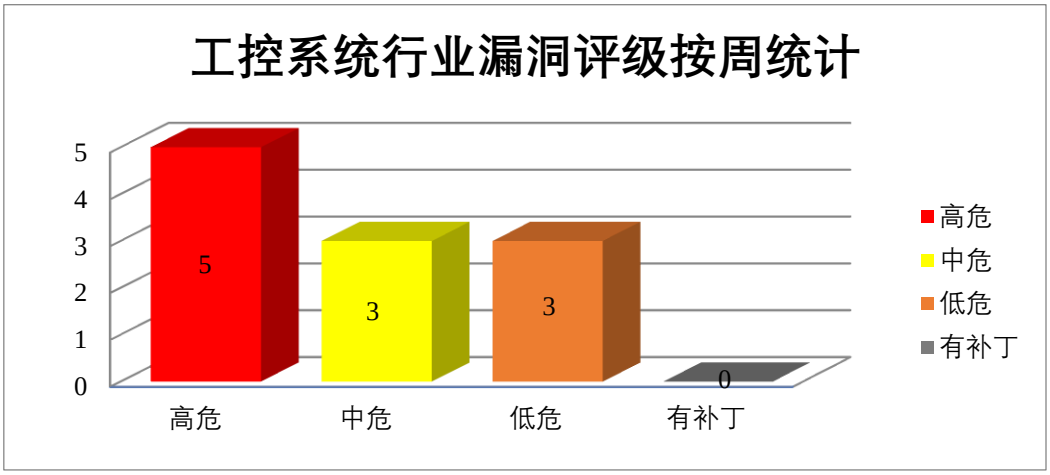

图 5 工控系统行业漏洞统计

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 和 Microsoft Windows Server 都是美国微软（Microsoft）公司的产品。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。Microsoft Windows DNS 是一个域名解析服务。Microsoft Windows Kernel 是 Windows 操作系统的内核。本周，上述产品被披露存在多个漏洞，攻击者可利用该漏洞实现远程代码执行。

CNVD 收录的相关漏洞包括：Microsoft Windows 和 Windows Server 远程代码执行漏洞（CNVD-2021-74287、CNVD-2021-74286、CNVD-2021-74285、CNVD-2021-74290、CNVD-2021-74289、CNVD-2021-74288）、Microsoft Windows Server 远程代码执行漏洞（CNVD-2021-74292、CNVD-2021-74291）。其中，“Microsoft Windows Server 远程代码执行漏洞（CNVD-2021-74291）”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-2021-74287

https://www.cnvd.org.cn/flaw/show/CNVD-2021-74286

https://www.cnvd.org.cn/flaw/show/CNVD-2021-74285

https://www.cnvd.org.cn/flaw/show/CNVD-2021-74290

https://www.cnvd.org.cn/flaw/show/CNVD-2021-74289

https://www.cnvd.org.cn/flaw/show/CNVD-2021-74288

https://www.cnvd.org.cn/flaw/show/CNVD-2021-74292

https://www.cnvd.org.cn/flaw/show/CNVD-2021-74291

2、 Adobe 产品安全漏洞

Adobe Bridge 是美国奥多比（Adobe）公司的一款文件查看器。Adobe Genuine Software Service 是一款正版软件服务。Adobe Illustrator 2021 是一款矢量绘图软件。Adobe Media Encoder 是一款视频和音频编码应用程序。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞在当前用户的上下文中执行任意代码，实现权限提升。

CNVD 收录的相关漏洞包括：Adobe Bridge 内存破坏漏洞（CNVD-2021-74107、CNVD-2021-74106）、Adobe Genuine Software Service 访问控制错误漏洞、Adobe Illustrator 2021 内存破坏漏洞（CNVD-2021-74110）、Adobe Illustrator 2021 操作系统命令注入漏洞、Adobe Media Encoder 内存越界访问漏洞（CNVD-2021-74111）、Adobe Bridge 越界写入漏洞（CNVD-2021-74117、CNVD-2021-74116）。其中，除 “Adobe Genuine Software Service 访问控制错误漏洞”外，其余漏洞的综合评级为“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-2021-74107
https://www.cnvd.org.cn/flaw/show/CNVD-2021-74106
https://www.cnvd.org.cn/flaw/show/CNVD-2021-74105
https://www.cnvd.org.cn/flaw/show/CNVD-2021-74110
https://www.cnvd.org.cn/flaw/show/CNVD-2021-74108
https://www.cnvd.org.cn/flaw/show/CNVD-2021-74111
https://www.cnvd.org.cn/flaw/show/CNVD-2021-74117
https://www.cnvd.org.cn/flaw/show/CNVD-2021-74116

3、 VMWare 产品安全漏洞

Vmware VMware vCenter Server 是美国威睿（Vmware）公司的一套服务器和虚拟化管理软件。该软件提供了一个用于管理 VMware vSphere 环境的集中式平台，可自动实施和交付虚拟基础架构。本周，上述产品被披露存在多个漏洞，攻击者可利用该漏洞在执行任意代码，获得对系统的未经授权访问，并执行未经身份验证的虚拟机网络设置操作，导致拒绝服务等。

CNVD 收录的相关漏洞包括：VMware vCenter Server 跨站脚本漏洞（CNVD-2021-74276）、VMware vCenter Server 代码执行漏洞、VMware vCenter Server 授权问题漏洞（CNVD-2021-74278、CNVD-2021-74284）、VMware vCenter Server 路径遍历漏洞、VMware vCenter Server 服务器端请求伪造漏洞、VMware vCenter Server 拒绝服务漏洞（CNVD-2021-74281、CNVD-2021-74280）。其中，“VMware vCenter Server 代码执行漏洞”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-2021-74276

https://www.cnvd.org.cn/flaw/show/CNVD-2021-74275

https://www.cnvd.org.cn/flaw/show/CNVD-2021-74278

https://www.cnvd.org.cn/flaw/show/CNVD-2021-74277

https://www.cnvd.org.cn/flaw/show/CNVD-2021-74282

https://www.cnvd.org.cn/flaw/show/CNVD-2021-74281

https://www.cnvd.org.cn/flaw/show/CNVD-2021-74280

https://www.cnvd.org.cn/flaw/show/CNVD-2021-74284

4、DELL 产品安全漏洞

Dell EMC PowerScale OneFS 是一款由 API 驱动的文件系统。本周，上述产品被披露存在多个漏洞，攻击者可利用该漏洞越权获取信息，提升权限等。

CNVD 收录的相关漏洞包括：Dell EMC PowerScale OneFS 信息泄露漏洞（CNVD-2021-73938、CNVD-2021-73939、CNVD-2021-73942）、Dell EMC PowerScale OneFS 日志记录不足漏洞、Dell EMC PowerScale OneFS OS 权限提升漏洞、Dell EMC PowerScale OneFS OS 命令注入漏洞、Dell EMC PowerScale OneFS 权限提升漏洞、Dell EMC PowerScale OneFS 权限分配不正确漏洞。其中，“Dell EMC PowerScale OneFS 权限提升漏洞”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-2021-73938

https://www.cnvd.org.cn/flaw/show/CNVD-2021-73937

https://www.cnvd.org.cn/flaw/show/CNVD-2021-73940

https://www.cnvd.org.cn/flaw/show/CNVD-2021-73939

https://www.cnvd.org.cn/flaw/show/CNVD-2021-73941

https://www.cnvd.org.cn/flaw/show/CNVD-2021-73943

https://www.cnvd.org.cn/flaw/show/CNVD-2021-73942

https://www.cnvd.org.cn/flaw/show/CNVD-2021-73945

5、PDFTools 空指针解引用漏洞

PDFTools 是一款将 PDF 文件转换为 ePUB 格式的工具。本周，PDFTools 被披露存在空指针解引用漏洞。攻击者可利用该漏洞导致拒绝服务。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-2021-73927

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	Dell EMC PowerScale OneF	高	厂商已发布了漏洞修复程序，请及

-73943	S 权限提升漏洞		时关注更新：https://www.dell.com/support/kbdoc/zh-cn/000190408/dsa-2021-142-dell-powerscale-onefs-security-update-for-multiple-vulnerabilities
CNVD-2021-74107	Adobe Bridge 内存破坏漏洞（CNVD-2021-74107）	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/bridge/apsb21-69.html
CNVD-2021-74106	Adobe Bridge 内存破坏漏洞（CNVD-2021-74106）	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/bridge/apsb21-69.html
CNVD-2021-74110	Adobe Illustrator 2021 内存破坏漏洞（CNVD-2021-74110）	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/illustrator/apsb21-42.html
CNVD-2021-74108	Adobe Illustrator 2021 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://helpx.adobe.com/security/products/illustrator/apsb21-42.html
CNVD-2021-74111	Adobe Media Encoder 内存越界访问漏洞（CNVD-2021-74111）	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/media-encoder/apsb21-70.html
CNVD-2021-74117	Adobe Bridge 越界写入漏洞（CNVD-2021-74117）	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/bridge/apsb21-53.html
CNVD-2021-74116	Adobe Bridge 越界写入漏洞（CNVD-2021-74116）	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/bridge/apsb21-53.html
CNVD-2021-74275	VMware vCenter Server 代码执行漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.vmware.com/security/advisories/VMSA-2021-0020.html
CNVD-2021-74291	Microsoft Windows Server 远程代码执行漏洞（CNVD-2021-74291）	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-2021-34458

小结：本周，Microsoft 产品被披露存在多个漏洞，攻击者可利用漏洞实现远程代码

执行。此外，Adobe、VMWare、DELL 等多款产品被披露存在多个漏洞，攻击者可利用漏洞越权获取信息，在当前用户的上下文中执行任意代码，实现权限提升等。另外，PDFTools 被披露存在空指针解引用漏洞。攻击者可利用该漏洞导致拒绝服务。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、Deskpro 跨站脚本漏洞

验证描述

Deskpro 是英国 Deskpro 公司的一套帮助台软件。该软件包括客户关系管理组件等，提供电子邮件、即时聊天和语音等功能。

Deskpro cloud 和 on-premise Deskpro 在 2021.1.6 之前版本中存在跨站脚本漏洞，该漏洞源于用户配置文件中的社交媒体链接缺乏输入验证，攻击者可通过该漏洞注入并在客户端执行 JavaScript 代码从而劫持 cookie 会话令牌。

验证信息

POC 链接：https://www.r29k.com/articles/bb/stored-xss-in-deskpro#anchor2

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2021-74295

信息提供者

新华三技术有限公司

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. 谷歌 Chrome 四个高危漏洞已更新

谷歌发布了安全更新，解决了适用于 Windows、Mac 和 Linux 的 Chrome 浏览器版本的四个高危漏洞。

参考链接：https://www.freebuf.com/news/291182.html

2. Apache 发布更新以修复一个被广泛利用的漏洞

Apache Software Foundation 已发布 HTTP Web Server 2.4.51，以解决一个被主动利用的路径遍历漏洞（CVE-2021-41773），该漏洞在之前的版本中仅部分解决。

参考链接：https://securityaffairs.co/wordpress/123096/hacking/apache-actively-exploited-flaw.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