国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2021 年 10 月 25 日-2021 年 10 月 31 日 **2021 年第 43 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 469 个，其中高危漏洞 86 个、中危漏洞 338 个、低危漏洞 45 个。漏洞平均分值为 5.31。本周收录的漏洞中，涉及 0day 漏洞 292 个（占 62%），其中互联网上出现“WordPress Pie Register 权限提升漏洞、WordPress 插件 Picture Gallery 'Edit Content URL'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 14569 个，与上周（7662 个）环比增加 90%。

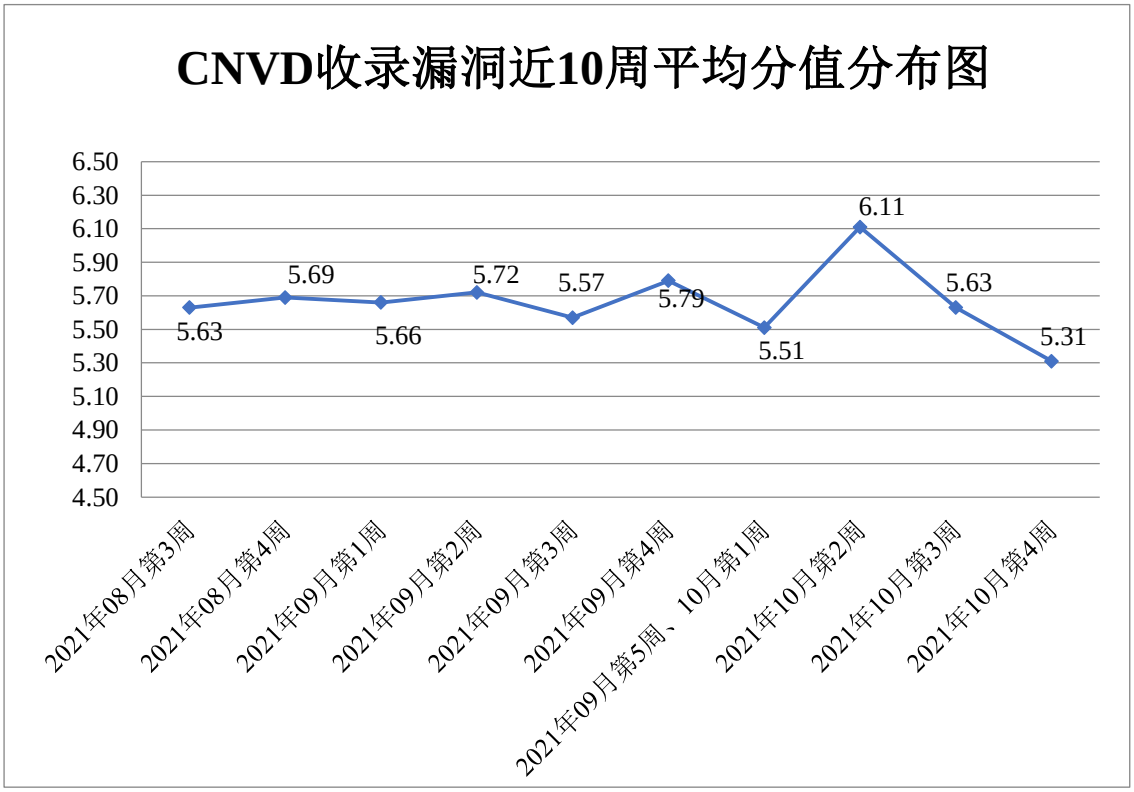

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 28 起，向基础电信企业通报漏洞事件 31 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 646 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 96 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：

珠海金山办公软件有限公司、珠海海鸟科技有限公司、珠海方诺信息科技有限公司、重庆泛普软件有限公司、中科博华信息科技有限公司、中国少年儿童新闻出版总社有限公司、正方软件股份有限公司、浙江大华技术股份有限公司、招商永隆银行有限公司、右鑫電子通信有限公司、友讯电子设备（上海）有限公司、亚信科技（成都）有限公司、兄弟（中国）商业有限公司、新天科技股份有限公司、新都（青岛）办公系统有限公司、西安新软信息科技有限公司、西安建大静态交通研究院有限公司、微星科技股份有限公司、微软（中国）有限公司、同望科技股份有限公司、天津天堰科技股份有限公司、拓维信息系统股份有限公司、宿迁鑫潮信息技术有限公司、苏州科达科技股份有限公司、世邦通信股份有限公司、石家庄捷搜网络科技有限公司、深圳英飞拓科技股份有限公司、深圳维盟科技股份有限公司、深圳市友华通信技术有限公司、深圳市网心科技有限公司、深圳市天翼软件有限公司、深圳市龙岗区沅陵网站服务店、深圳市惠尔顿信息技术有限公司、深圳市华波美通信技术有限公司、深圳市超时代软件有限公司、深圳前海百递网络有限公司、上海商派网络科技有限公司、上海蓝山办公软件有限公司、上海会畅通讯股份有限公司、上海华测导航技术股份有限公司、上海海海计算机软件有限公司、上海孚盟软件有限公司、上海二三四五网络控股集团股份有限公司、山西龙采科技有限公司晋中分公司、山西单点科技有限公司、山东顺能网络科技有限公司、厦门四信通信科技有限公司、厦门市灵鹿谷科技有限公司、厦门海为科技有限公司、瑞斯康达科技发展股份有限公司、南通艾睦网络科技有限公司、南宁旭东网络科技有限公司、茉柏枘（上海）软件科技有限公司、眉山市爱客网络科技有限公司、洛阳云业信息科技有限公司、龙江银行股份有限公司、龙采科技（山西）有限公司、朗坤智慧科技股份有限公司、金蝶软件（中国）有限公司、江西铭软科技有限公司、佳能（中国）有限公司、惠普贸易（上海）有限公司、杭州中宝科技有限公司、杭州雄伟科技开发股份有限公司、杭州海康威视数字技术股份有限公司、汉中紫柏云旅文化旅游股份有限公司、海南驰豹科技有限公司、海尔集团电子商务有限公司、哈尔滨伟成科技有限公司、桂林崇胜网络科技有限公司、高新兴科技集团股份有限公司、福州网钛软件科技有限公司、佛山市顺德区出格软件设计有限公司、得捷电子（上海）有限公司、戴尔（中国）有限公司、成都卓越远扬信息技术有限公司、成都万江港利科技股份有限公司、成都借宝科技有限公司、成都海

翔软件有限公司、北京云章科技有限公司、北京云帆互联科技有限公司、北京易普拉格科技股份有限公司、北京亚控科技发展有限公司、北京小米科技有限责任公司、北京我知科技有限公司、北京停简单信息技术有限公司、北京润尼尔网络科技有限公司、北京派网软件有限公司、北京杰控科技有限公司、北京宏业超世纪科技有限公司、安徽渔之蓝教育软件技术有限公司、安徽旭帆信息科技有限公司、安徽南瑞继远电网技术有限公司、安徽富煌科技股份有限公司、《中国学术期刊（光盘版）》电子杂志社有限公司、阿里巴巴集团安全应急响应中心、联想全球安全实验室、京东云安全、易迅软件工作室、天翔网络、梦想 CMS、Lexmark、XnSoft、VMware, Inc.、Sumatra PDF、Q-SEE、Oracle、InvestinTech、INFRAWARE、Dreamer CMS 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，北京神州绿盟科技有限公司、北京天融信网络安全技术有限公司、北京数字观星科技有限公司、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、广东蓝爵网络安全技术股份有限公司、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 、北京信联科汇科技有限公司、南京众智维信息科技有限公司、杭州海康威视数字技术股份有限公司、京东云安全、杭州迪普科技股份有限公司、长春嘉诚信息技术股份有限公司、新疆海狼科技有限公司、河南信安世纪科技有限公司、内蒙古云科数据服务股份有限公司、重庆都会信息科技有限公司、北京惠而特科技有限公司、北京大学、内蒙古洞明科技有限公司、福建省海峡信息技术有限公司、北京云科安信科技有限公司（Seraph 安全实验室）、南京树安信息技术有限公司、北京远禾科技有限公司、浙江木链物联网科技有限公司、博智安全科技股份有限公司、北京安帝科技有限公司、山石网科通信技术股份有限公司、百度 AIoT 安全团队、中国烟草总公司湖北省公司、星云博创科技有限公司、天讯瑞达通信技术有限公司、北京水木羽林科技有限公司、中国—东盟信息港股份有限公司、奇安信-工控安全实验室、北京君云天下科技有限公司、华泰人寿保险股份有限公司、北京科技大学、北京威努特技术有限公司、华润（集团）有限公司及其他个人白帽子向 CNVD 提交了 14569 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 10994 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）	6966	6966
斗象科技（漏洞盒子）	3421	3421

上海交大	607	607
北京神州绿盟科技有限公司	367	11
北京奇虎科技有限公司	323	323
北京天融信网络安全技术有限公司	327	19
北京数字观星科技有限公司	281	0
哈尔滨安天科技集团股份有限公司	269	0
新华三技术有限公司	178	0
华为技术有限公司	151	0
深信服科技股份有限公司	100	0
恒安嘉新（北京）科技股份公司	60	0
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	58	3
远江盛邦（北京）网络安全科技股份有限公司	56	0
南京联成科技发展股份有限公司	33	0
西安四叶草信息技术有限公司	6	0
北京安信天行科技有限公司	3	0
北京知道创宇信息技术有限公司	2	0
山东云天安全技术有限公司	725	725
广东蓝爵网络安全技术股份有限公司	451	451
联想全球安全实验室	373	0
北京山石网科信息技术有限公司	230	230
北京华顺信安科技有限公司	117	0
河南灵创电子科技有限公司	106	106
北京信联科汇科技有	105	105

限公司		
南京众智维信息科技有限公司	100	100
杭州海康威视数字技术股份有限公司	78	78
京东云安全	54	54
杭州迪普科技股份有限公司	45	15
长春嘉诚信息技术股份有限公司	35	35
新疆海狼科技有限公司	32	32
河南信安世纪科技有限公司	32	32
内蒙古云科数据服务股份有限公司	29	29
亚信科技（成都）有限公司	28	0
重庆都会信息科技有限公司	19	19
北京惠而特科技有限公司	16	16
北京大学	14	14
内蒙古洞明科技有限公司	12	12
福建省海峡信息技术有限公司	8	8
北京云科安信科技有限公司（Seraph 安全实验室）	8	8
南京树安信息技术有限公司	8	8
北京远禾科技有限公司	7	7
浙江木链物联网科技有限公司	6	6
博智安全科技股份有限公司	5	5
北京安帝科技有限公司	4	4
山石网科通信技术股份有限公司	4	4
百度 AIoT 安全团队	3	3

中国烟草总公司湖北省公司	3	3
星云博创科技有限公司	3	3
天讯瑞达通信技术有限公司	3	3
北京水木羽林科技有限公司	3	3
中国—东盟信息港股份有限公司	2	2
奇安信-工控安全实验室	2	2
北京君云天下科技有限公司	1	1
华泰人寿保险股份有限公司	1	1
北京科技大学	1	1
北京威努特技术有限公司	1	1
华润（集团）有限公司	1	1
CNCERT 浙江分中心	4	4
个人	1088	1088
报送总计	17034	14569

本周漏洞按类型和厂商统计

本周，CNVD 收录了 469 个漏洞。应用程序 153 个，WEB 应用 109 个，网络设备（交换机、路由器等网络端设备）102 个，数据库 43 个，智能设备（物联网终端设备）37 个，操作系统 17 个，安全产品 8 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	153
WEB 应用	109
网络设备（交换机、路由器等网络端设备）	102
数据库	43
智能设备（物联网终端设备）	37
操作系统	17
安全产品	8

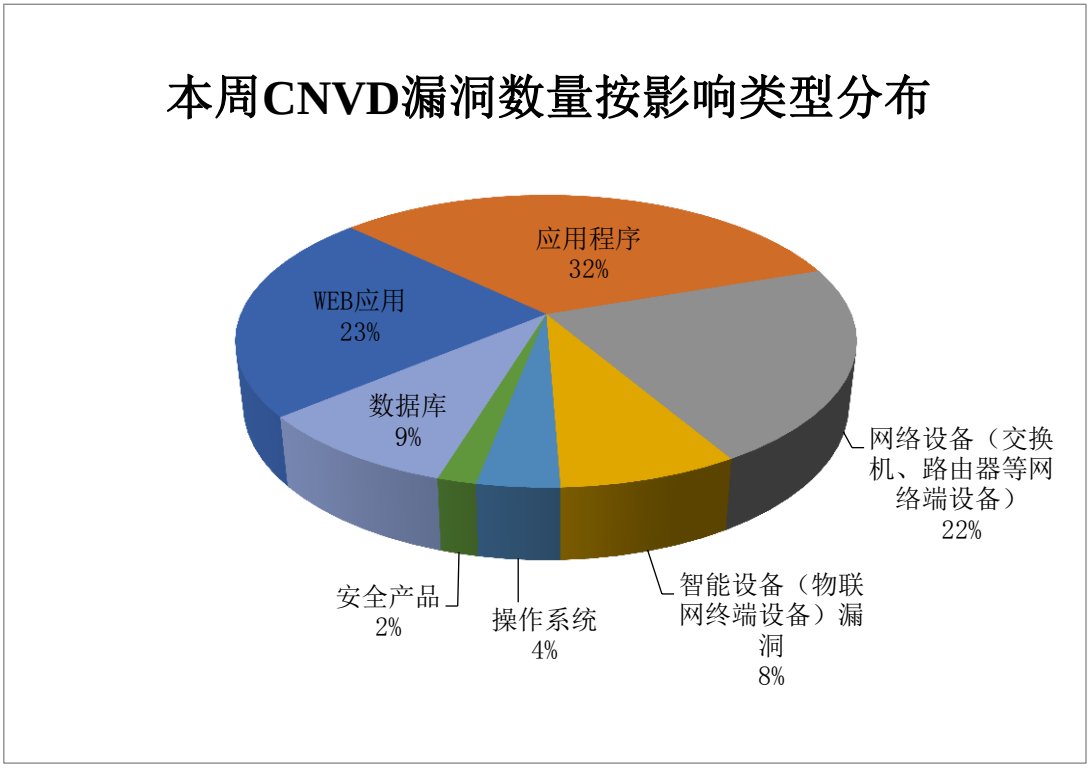

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 D-Link、Oracle、Lexmark 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	75	16%
2	Oracle	72	15%
3	Lexmark	19	4%
4	HPE	15	3%
5	GPAC	13	3%
6	Adobe	13	3%
7	Cisco	12	3%
8	DedeCMS	10	2%
9	Radare	9	2%
10	其他	231	49%

本周行业漏洞收录情况

本周，CNVD 收录了 102 个电信行业漏洞，15 个移动互联网行业漏洞，4 个工控行业漏洞（如下图所示）。其中，“Cisco IOS XE SD-WAN Software 命令注入漏洞、Google Android 权限提升漏洞（CNVD-2021-80274）、Advantech WebAccess 堆缓冲区溢出漏洞”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/

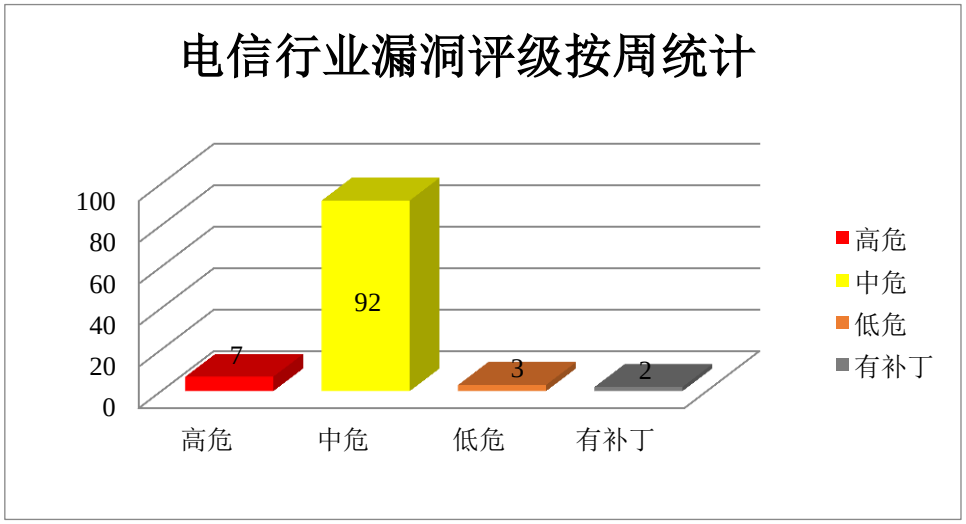

图 3 电信行业漏洞统计

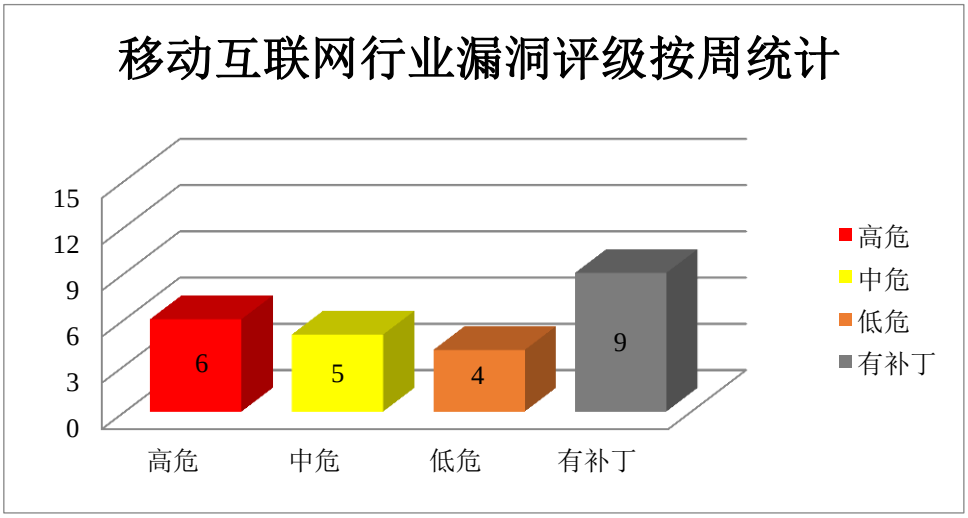

图 4 移动互联网行业漏洞统计

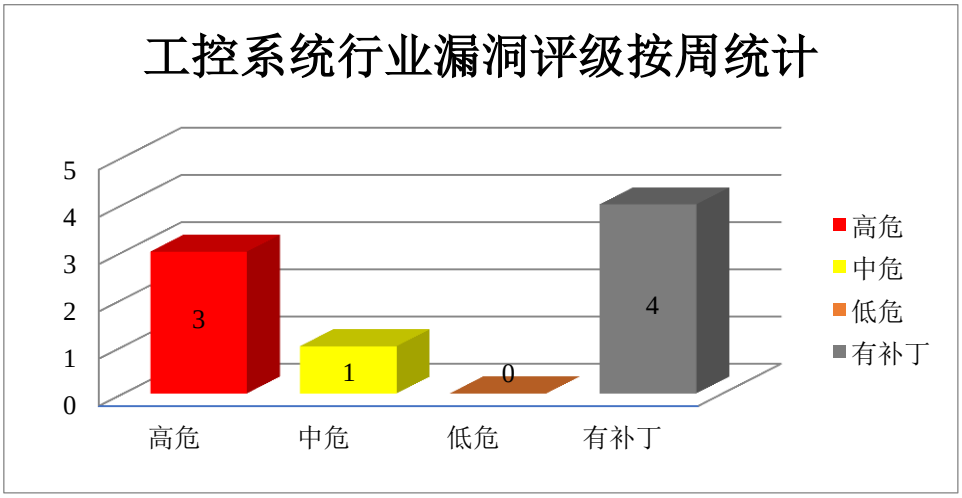

图 5 工控系统行业漏洞统计

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、Adobe 产品安全漏洞

Adobe Photoshop，简称“PS”，是由 Adobe 公司开发和发行的图像处理软件。Adobe XMP Toolkit SDK 可让您将 XMP 功能集成到您的产品或解决方案中。Adobe Experience Manager 是一款企业内容管理解决方案，可帮助您简化内容和资产的管理和投放。Adobe Genuine Service 是一项免费服务，可定期验证您计算机上的 Adobe 应用程序是否为正版，如果不是，则通知客户。Adobe Digital Editions 软件提供一种引人入胜的方式帮助您查看和管理 eBooks 和其它数字出版物。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，提升权限，执行任意代码等。

CNVD 收录的相关漏洞包括：Adobe Photoshop 缓冲区溢出漏洞（CNVD-2021-79743）、Adobe XMP Toolkit SDK 越界读取漏洞（CNVD-2021-79742）、Adobe Experience Manager 跨站脚本漏洞（CNVD-2021-79744、CNVD-2021-79748）、Adobe Genuine Service 权限提升漏洞、Adobe Digital Editions 任意文件系统写入漏洞、Adobe Digital Editions OS 命令注入漏洞（CNVD-2021-79749）、Adobe Digital Editions 权限提升漏洞（CNVD-2021-79751）。其中，“Adobe Photoshop 缓冲区溢出漏洞（CNVD-2021-79743）、Adobe Digital Editions OS 命令注入漏洞（CNVD-2021-79749）”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-2021-79743

https://www.cnvd.org.cn/flaw/show/CNVD-2021-79742

https://www.cnvd.org.cn/flaw/show/CNVD-2021-79744

https://www.cnvd.org.cn/flaw/show/CNVD-2021-79747

https://www.cnvd.org.cn/flaw/show/CNVD-2021-79748

https://www.cnvd.org.cn/flaw/show/CNVD-2021-79750

https://www.cnvd.org.cn/flaw/show/CNVD-2021-79749

https://www.cnvd.org.cn/flaw/show/CNVD-2021-79751

2、Cisco 产品安全漏洞

Cisco IOS XE SD-WAN Software 是美国思科（Cisco）公司的一款应用于 Cisco IOS XE 网络操作系统的用于网络管理（软件定义网络）的软件。Cisco IOS 是一套为其网络设备开发的操作系统。Cisco IOS XE Software 是一个操作系统。用于企业有线和无线访问，汇聚，核心和 WAN 的单一操作系统，Cisco IOS XE 降低了业务和网络的复杂性。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞重新加载受影响的设备，执行任意命令，导致拒绝服务等。

CNVD 收录的相关漏洞包括：Cisco IOS XE SD-WAN Software 命令注入漏洞、Cisco IOS XE Software 拒绝服务漏洞（CNVD-2021-80662、CNVD-2021-80665、CNVD-2021-80663）、Cisco IOS XE Software 身份验证绕过漏洞、Cisco IOS XE Software 访问控制错误漏洞（CNVD-2021-80664）、Cisco IOS 和 Cisco IOS XE Software 拒绝服务漏洞（CNVD-2021-80669、CNVD-2021-80666）。其中，“Cisco IOS XE SD-WAN Software 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-2021-80658

https://www.cnvd.org.cn/flaw/show/CNVD-2021-80662

https://www.cnvd.org.cn/flaw/show/CNVD-2021-80660

https://www.cnvd.org.cn/flaw/show/CNVD-2021-80665

https://www.cnvd.org.cn/flaw/show/CNVD-2021-80664

https://www.cnvd.org.cn/flaw/show/CNVD-2021-80663

https://www.cnvd.org.cn/flaw/show/CNVD-2021-80669

https://www.cnvd.org.cn/flaw/show/CNVD-2021-80666

3、Oracle 产品安全漏洞

Oracle MySQL Server 是美国甲骨文（Oracle）公司的一款关系型数据库。本周，上述产品被披露存在输入验证错误漏洞，攻击者可利用漏洞操纵数据，执行拒绝服务（DoS）攻击。

CNVD 收录的相关漏洞包括：Oracle MySQL Server 输入验证错误漏洞（CNVD-2021-80244、CNVD-2021-80242、CNVD-2021-80247、CNVD-2021-80246、CNVD-2021-80245、CNVD-2021-80250、CNVD-2021-80249、CNVD-2021-80248）。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-2021-80244

https://www.cnvd.org.cn/flaw/show/CNVD-2021-80242

https://www.cnvd.org.cn/flaw/show/CNVD-2021-80247

https://www.cnvd.org.cn/flaw/show/CNVD-2021-80246

https://www.cnvd.org.cn/flaw/show/CNVD-2021-80245

https://www.cnvd.org.cn/flaw/show/CNVD-2021-80250

https://www.cnvd.org.cn/flaw/show/CNVD-2021-80249

https://www.cnvd.org.cn/flaw/show/CNVD-2021-80248

4、HPE 产品安全漏洞

HPE Aruba ClearPass Policy Manager 是一个网络访问控制（NAC）解决方案。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞越权访问 web 界面的敏感信息，提升权限，执行任意命令。

CNVD 收录的相关漏洞包括：HPE Aruba ClearPass Policy Manager 远程命令注入漏洞（CNVD-2021-80165、CNVD-2021-80164、CNVD-2021-80166、CNVD-2021-80177）、HPE Aruba ClearPass Policy Manager 信息泄露漏洞（CNVD-2021-80163、CNVD-2021-80169）、HPE Aruba ClearPass Policy Manager 本地权限提升漏洞、HPE Aruba ClearPass Policy Manager 远程目录遍历漏洞。其中，除“HPE Aruba ClearPass Policy Manager 信息泄露漏洞（CNVD-2021-80163）、CNVD-2021-80169）”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-2021-80165

https://www.cnvd.org.cn/flaw/show/CNVD-2021-80164

https://www.cnvd.org.cn/flaw/show/CNVD-2021-80163

https://www.cnvd.org.cn/flaw/show/CNVD-2021-80169

https://www.cnvd.org.cn/flaw/show/CNVD-2021-80168

https://www.cnvd.org.cn/flaw/show/CNVD-2021-80167

https://www.cnvd.org.cn/flaw/show/CNVD-2021-80166

https://www.cnvd.org.cn/flaw/show/CNVD-2021-80177

5、Projectsend 目录遍历漏洞

ProjectSend 是一款免费、面向客户的私有文件共享 Web 应用程序。本周，Projectsend 被披露存在目录遍历漏洞。该漏洞源于对 files[]参数的输入缺少验证。攻击者可利用漏洞通过添加../将所有 PHP 文件或系统上有权访问的任何文件移动到/upload/files/文件夹。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-2021-81765

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-2021-80274	Google Android 权限提升漏洞（CNVD-2021-80274）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://source.android.com/security/bulletin/2021-10-01
CNVD-2021-79775	Dell EMC iDRAC9 不当认证漏洞	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/zh-cn/000186420/dsa-2021-082-dell-emc-idrac-9-security-update-for-improper-authentication-vulnerability
CNVD-2021-80283	HTMLDOC 资源管理错误漏洞	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/michaelrsweet/htmldoc/issues/414
CNVD-2021-80266	Advantech WebAccess 堆栈缓冲区溢出漏洞（CNVD-2021-80266）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://us-cert.cisa.gov/ics/advisories/icsa-21-285-02
CNVD-2021-80269	TinyFileManager 跨站请求伪造漏洞	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/prasathmani/tinyfilemanager
CNVD-2021-80267	Advantech WebAccess 堆缓冲区溢出漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://us-cert.cisa.gov/ics/advisories/icsa-21-285-02
CNVD-2021-80277	Google Android 权限提升漏洞（CNVD-2021-80277）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://source.android.com/security/bulletin/2021-10-01
CNVD-2021-80281	HTMLDOC 堆缓冲区溢出漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://github.com/michaelrsweet/htmldoc/issues/412
CNVD-2021-81812	Oracle Java SE 和 Oracle GraalVM Enterprise Edition 信息泄露漏洞（CNVD-2021-81812）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.oracle.com/security-alerts/cpuoct2021.html
CNVD-2021	Advantech WebAccess 堆栈	高	厂商已发布了漏洞修复程序，请及

-80272	缓冲区溢出漏洞（CNVD-2021-80272）		时关注更新：https://www.advantech.com/support/details/installation?id=1-MS9MJV

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，提升权限，执行任意代码等。此外，Cisco、Oracle、HPE 等多款产品被披露存在多个漏洞，攻击者可利用漏洞越权访问 web 界面的敏感信息，提升权限，执行任意命令，导致拒绝服务等。另外，Projectsend 被披露存在目录遍历漏洞。攻击者可利用漏洞通过添加../将所有 PHP 文件或系统上有权访问的任何文件移动到/upload/files/文件夹。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 Pie Register 权限提升漏洞

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 Pie Register 存在权限提升漏洞。攻击者可利用该漏洞获取提升的权限。

验证信息

POC 链接：https://packetstormsecurity.com/files/164446/WordPress-Pie-Register-3.7.1.4-Privilege-Escalation.html

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2021-81764

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. 微软发现 macOS 中存在 Shrootless 漏洞

微软发现 macOS 中存在一个被称为 Shrootless（CVE-2021-30892）的漏洞，它可以让攻击者绕过系统的完整性保护。

参考链接：https://securityaffairs.co/wordpress/123898/hacking/macos-shrootless-cve-2021-30892-flaw.html

2. 超过 100 万 WordPress 网站受到 OptinMonster 插件缺陷影响

OptinMonster 插件中存在一个高严重性漏洞（CVE-2021-39341），可能允许在 WordPress 网站上出现未经授权的 API 访问。

参考链接：https://securityaffairs.co/wordpress/123886/hacking/wordpress-optinmonster-plugin-flaws.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