国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2021 年 02 月 08 日-2021 年 02 月 21 日　　2021 年第6、7 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 426 个，其中高危漏洞 194 个、中危漏洞 183 个、低危漏洞 49 个。漏洞平均分值为 6.10。本周收录的漏洞中，涉及 0day 漏洞 231 个（占 54%），其中互联网上出现“Oscar Arzola PressBooks 跨站脚本漏洞、Gym Management System SQL 注入漏洞（CNVD-2021-11281）”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 4438 个，与上周（6601 个）环比减少 33%。

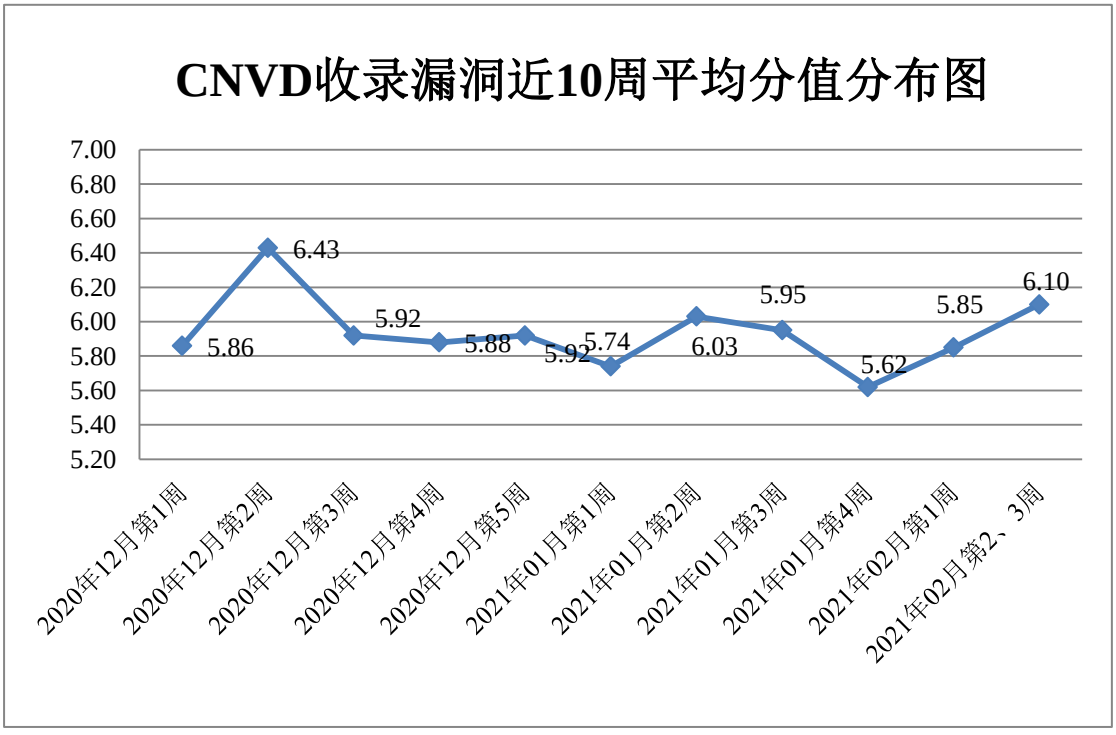

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 14 起，向基础电信企业通报漏洞事件 13 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 405 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 63 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 13 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：

郑州易盛信息技术有限公司、快排 CMS、北京一诺互联科技有限公司、珠海金山办公软件有限公司、上海纵之格科技有限公司、合肥明靖信息科技有限公司、杭州凯凯科技有限公司、常州贞明电子科技有限公司、广州网易计算机系统有限公司、苏州聚尚网络科技有限公司、中航证券有限公司、朋友圈网络科技有限公司、财信证券有限责任公司、济南博麟网络科技有限公司、南京越博动力系统股份有限公司、ZZCMS、湖北淘码千维信息科技有限公司、广州市互诺计算机科技有限公司、北京传奇华育教育科技股份有限公司、广州中海达卫星导航技术股份有限公司、上海盛代信息科技有限公司、江西金格科技股份有限公司、福建省华渔教育科技有限公司、杭州橙诺科技有限公司、广州思迈特软件有限公司、米酷影视、苹果 CMS、武汉金同方科技有限公司、SeaCMS、上海依图网络科技有限公司、财通证券股份有限公司、上海牛之云网络科技有限公司、深圳市大世同舟信息科技有限公司、广州市创科网络科技有限公司、深圳市进云软件科技有限公司、华泰证券股份有限公司、中泰证券股份有限公司、浙江宇视科技有限公司、中科博华信息科技有限公司、杭州海康威视数字技术股份有限公司、广州鼎成信息科技有限公司、上海锋趣网络科技有限公司、海信集团有限公司、北京网易有道计算机系统有限公司、杭州米络星科技（集团）有限公司、二六三网络通信股份有限公司、深圳市财富趋势科技股份有限公司、海洋 CMS、深圳市微客互动有限公司、北京艺龙信息技术有限公司、中国储备粮管理集团有限公司、上海泛微网络科技股份有限公司、施耐德电气(中国)有限公司、北京云帆互联科技有限公司、新时代证券股份有限公司、Hsycms、《中国学术期刊（光盘版）》电子杂志社有限公司、中兴通讯股份有限公司、华宝证券有限责任公司、渤海证券股份有限公司、东营金石软件有限公司、国盛证券、荆州市华诚网络信息技术有限公司、河北赫烁科技有限公司、厦门科拓通讯技术股份有限公司、浙江慕枫网站科技有限公司、西部动力（北京）科技有限公司、广州齐博网络科技有限公司、漳州市芗城帝兴软件开发有限公司、广发证券股份有限公司、长城证券股份有限公司、西部证券股份有限公司、光大证券股份有限公司、中银国际证券股份有限公司、信达证券股份有限公司、粤开证券股份有限公司、首创证券股份有限公司、东海证券股份有限公司、国融证券股份有限公司、上海证券有限责任公司、金元证券股份有限公司、国金证券股份有限公司、金蝶软件、西南证券股份有限公司、广州本盈计算机科技有限公司、陕西亚皇科技有限公司、深圳市皓峰通讯技术有限公司、浙江慕枫网络科技有限公司、成都零起飞网络、博世（中国）投资有限公司、海盐创宜软件科技有限公司、OPTO22、

北京转折文化发展有限公司、屏通科技股份有限公司、山西牛酷信息科技有限公司、上海百胜软件股份有限公司、锐捷网络股份有限公司、Cesanta 软件公司、瑞安市优博科技有限公司、北京爱奇艺科技有限公司、北京映翰通网络技术股份有限公司、瑞安市商企网络科技有限公司、云南华企优享网络科技有限公司、温州乔宇科技有限公司、畅捷通信息技术股份有限公司、北京同联信息技术有限公司、广东广凌信息科技股份有限公司、北京五指互联科技有限公司、国都证券股份有限公司、杭州当虹科技股份有限公司、万兴科技集团股份有限公司、杭州故乡人网络科技有限公司、浙江大华技术股份有限公司、青岛灼灼文化传媒有限公司、武汉沃讯科技有限公司、济南宇霞信息技术有限公司、上海迈微软件科技有限公司、北京多点在线科技有限公司、成都卓越远扬信息技术有限公司、杭州安恒信息技术股份有限公司、上海畅指网络科技有限公司、深圳齐心好视通云计算有限公司、正方软件股份有限公司、北京博思汇信息技术有限公司、海通证券股份有限公司、广州市花都区新华伟创广告设计服务部、思科系统（中国）网络技术有限公司、广州视臻信息科技有限公司、网易、陌陌安全应急响应中心、沈阳数业信息技术有限公司、保定市互动企业营销策划有限公司、内蒙古浩海商贸有限公司、佛山市搜虎网络科技有限公司、深圳市友华通信技术有限公司、Catfish、爱普生（中国）有限公司、微软（中国）有限公司和深圳市吉祥腾达科技有限公司。

本周，CNVD 发布了《关于微软 Windows 操作系统存在 TCP/IP 高危漏洞的安全公告》。详情参见 CNVD 网站公告内容。

https://www.cnvd.org.cn/webinfo/show/6051

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，北京山石网科信息技术有限公司、上海犀点意象网络科技有限公司、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 、北京华云安信息技术有限公司、北京天地和兴科技有限公司、山东云天安全技术有限公司、安徽长泰信息安全服务有限公司、山东华鲁科技发展股份有限公司、国瑞数码零点实验室、河南信安世纪科技有限公司、重庆贝特计算机系统工程有限公司、杭州海康威视数字技术股份有限公司、贵州多彩宝互联网服务有限公司、小安（北京）科技有限公司、星云博创科技有限公司、远江盛邦（北京）网络安全科技股份有限公司、北京国舜科技股份有限公司、北京长亭科技有限公司、北京君云天下科技有限公司、北京云科安信科技有限公司（Seraph 安全实验室）、上海纽盾科技股份有限公司、武汉明嘉信信息安全检测评估有限公司、北京远禾科技有限公司、广西等保安全测评有限公司、泽鹿安全、北京时代新威信息技术有限公司、北京顶象技术有限公司、北京圣博润高新技术股份有限公司、北京信联科汇科技有限公司、上海嵴函信息科技有限公司、信联科技（南京）有限公司、北京时代新威信息技术有限公司、广州安亿信软件科技有限公司、国网山东

省电力公司、吉林谛听信息技术有限公司、南水北调中线信息科技有限公司、平安银河实验室、山东新潮信息技术有限公司、郑州云智信安安全技术有限公司、中国工商银行软件开发中心及其他个人白帽子向 CNVD 提交了 4438 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 3228 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	原创漏洞数量
斗象科技（漏洞盒子）	1472	1472
上海交大	1158	1158
奇安信网神（补天平台）	598	598
华为技术有限公司	217	0
哈尔滨安天科技集团股份有限公司	115	0
新华三技术有限公司	68	0
中国电信集团系统集成有限责任公司	68	68
北京数字观星科技有限公司	24	0
杭州迪普科技股份有限公司	21	0
中国电信股份有限公司网络安全产品运营中心	20	0
北京华顺信安科技有限公司	1	0
北京知道创宇信息技术股份有限公司	1	0
北京山石网科信息技术有限公司	102	102
上海犀点意象网络科技有限公司	75	75
南京众智维信息科技有限公司	73	73
河南灵创电子科技有限公司	66	66
北京华云安信息技术有限公司	56	56
北京天地和兴科技有限公司	49	49
山东云天安全技术有限公司	49	49
安徽长泰信息安全服务有限公司	42	42
山东华鲁科技发展股份有限公司	33	33
国瑞数码零点实验室	24	24
河南信安世纪科技有限公司	21	21
重庆贝特计算机系统工程有	20	20

限公司		
杭州海康威视数字技术股份有限公司	12	12
贵州多彩宝互联网服务有限公司	11	11
小安（北京）科技有限公司	11	11
星云博创科技有限公司	10	10
远江盛邦（北京）网络安全科技股份有限公司	10	10
北京国舜科技股份有限公司	6	6
北京长亭科技有限公司	5	5
北京君云天下科技有限公司	4	4
北京云科安信科技有限公司（Seraph 安全实验室）	4	4
上海纽盾科技股份有限公司	4	4
武汉明嘉信信息安全检测评估有限公司	4	4
北京远禾科技有限公司	3	3
广西等保安全测评有限公司	3	3
泽鹿安全	3	3
北京时代新威信息技术有限公司	3	3
北京顶象技术有限公司	2	2
北京圣博润高新技术股份有限公司	2	2
北京信联科汇科技有限公司	2	2
上海崤函信息科技有限公司	2	2
信联科技（南京）有限公司	2	2
北京时代新威信息技术有限公司	1	1
广州安亿信软件科技有限公司	1	1
国网山东省电力公司	1	1
吉林谛听信息技术有限公司	1	1
南水北调中线信息科技有限公司	1	1
平安银河实验室	1	1
山东新潮信息技术有限公司	1	1
郑州云智信安安全技术有限公司	1	1
中国工商银行软件开发中心	1	1
CNCERT 海南分中心	6	6
CNCERT 山西分中心	5	5

CNCERT 青海分中心	3	3
CNCERT 贵州分中心	1	1
CNCERT 四川分中心	1	1
个人	404	404
报送总计	4905	4438

本周漏洞按类型和厂商统计

本周，CNVD 收录了 426 个漏洞。应用程序 214 个，WEB 应用 110 个，网络设备（交换机、路由器等网络端设备）59 个，操作系统 32 个，智能设备（物联网终端设备）9 个，安全产品 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
应用程序	214
WEB 应用	110
网络设备（交换机、路由器等网络端设备）	59
操作系统	32
智能设备（物联网终端设备）	9
安全产品	2

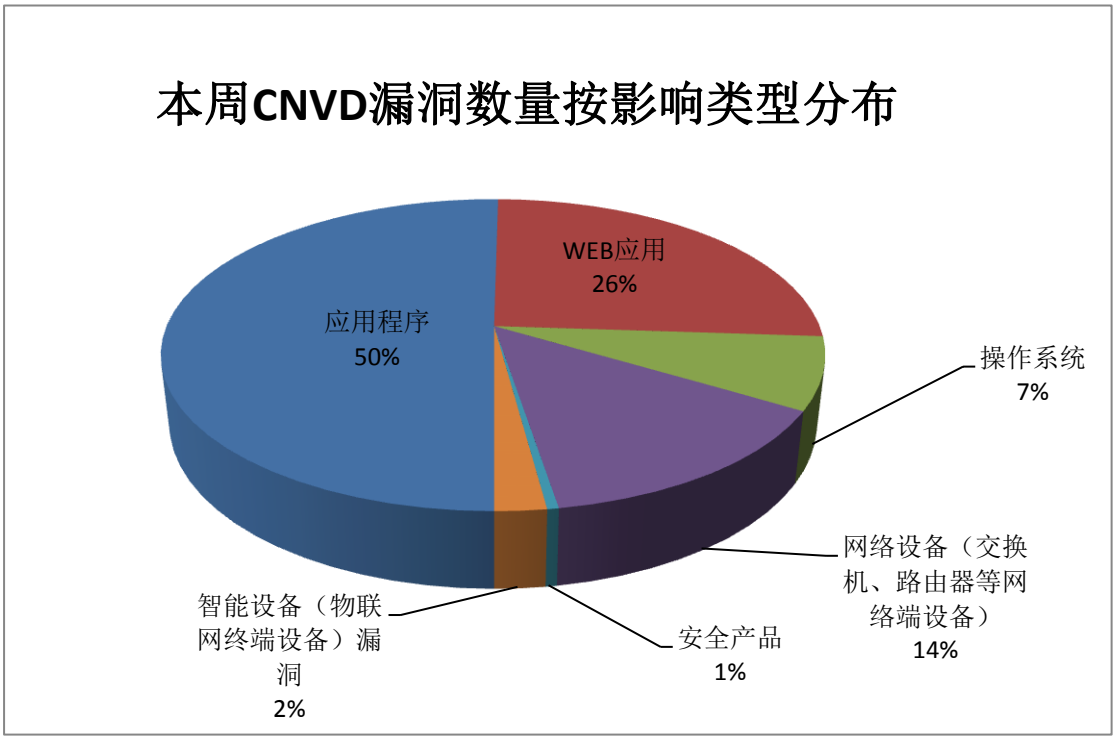

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Intel、Google、IBM 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	Intel	28	7%
2	Google	26	6%
3	IBM	20	5%
4	成都奇鲁科技有限公司&成都安易迅科技有限公司	19	4%
5	Cisco	17	4%
6	Adobe	16	4%
7	HPE	14	3%
8	北京映翰通网络技术股份有限公司	13	3%
9	TP-LINK	12	3%
10	其他	261	61%

本周行业漏洞收录情况

本周，CNVD 收录了 60 个电信行业漏洞，20 个移动互联网行业漏洞，2 个工控行业漏洞（如下图所示）。其中，“Advantech iView 关键功能缺少认证漏洞、 Google Android wlan driver 越界写漏洞、Google Android VPU 权限提升漏洞（CNVD-2021-09904）、Google Android display driver 限提升漏洞、Google Android mtkpower 内存破坏漏洞”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/

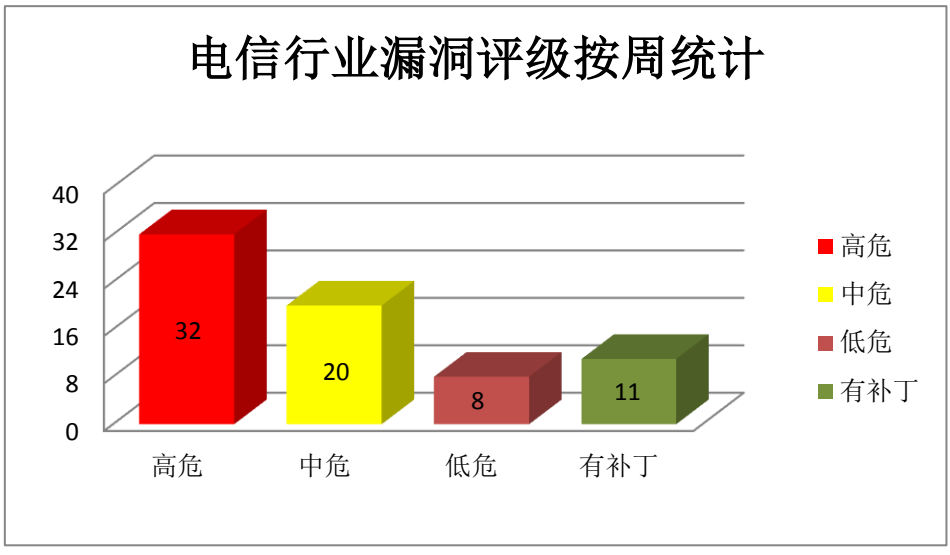

图 3 电信行业漏洞统计

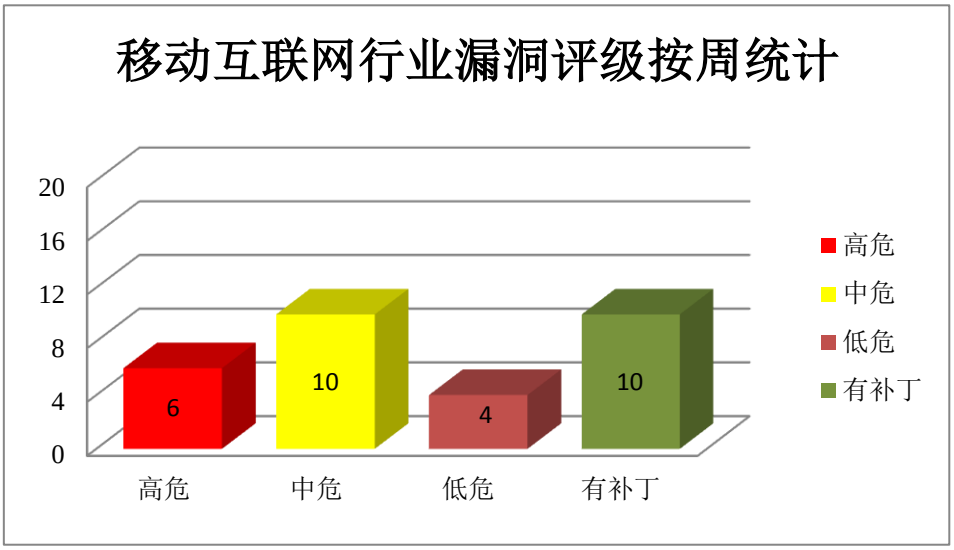

图 4 移动互联网行业漏洞统计

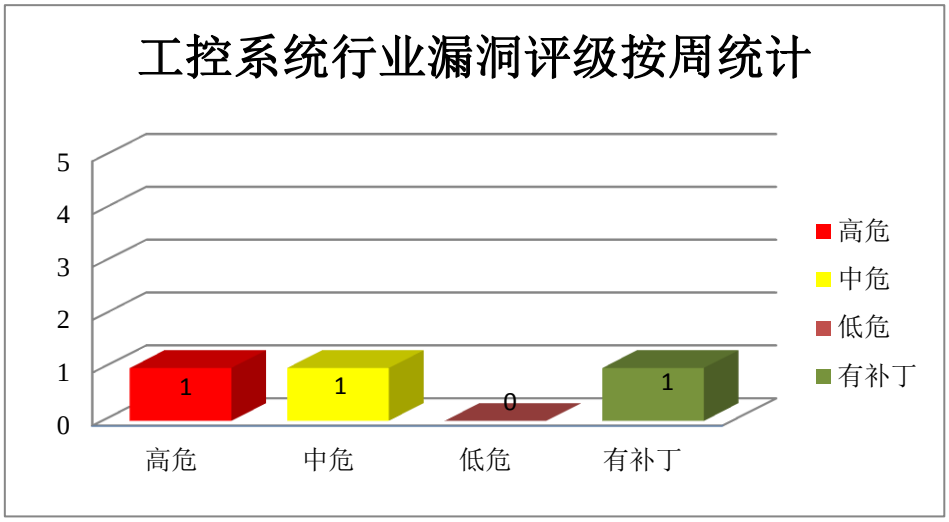

图 5 工控系统行业漏洞统计

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、Google 产品安全漏洞

Google Android 是美国谷歌（Google）和开放手持设备联盟（简称 oha）的一套以 Linux 为基础的开源操作系统。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞导致需要系统执行特权的权限本地升级，提交特殊的请求，可提升权限，导致拒绝服务等。

CNVD 收录的相关漏洞包括：Google Android VPU 权限提升漏洞（CNVD-2021-09904、CNVD-2021-09908）、Google Android wlan driver 越界写漏洞、Google Android

mtkpower 内存破坏漏洞、Google Android display driver 限提升漏洞、Google Android Framework 拒绝服务漏洞（CNVD-2021-10540）、Google Android Pixel 权限提升漏洞（CNVD-2021-10541）、Google Android 资源管理错误漏洞（CNVD-2021-10538）。其中，“Google Android VPU 权限提升漏洞（CNVD-2021-09904、CNVD-2021-09908）、Google Android wlan driver 越界写漏洞、Google Android mtkpower 内存破坏漏洞、Google Android display driver 限提升漏洞、Google Android Framework 拒绝服务漏洞（CNVD-2021-10540）、Google Android Pixel 权限提升漏洞（CNVD-2021-10541）”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-2021-09904

https://www.cnvd.org.cn/flaw/show/CNVD-2021-09903

https://www.cnvd.org.cn/flaw/show/CNVD-2021-09908

https://www.cnvd.org.cn/flaw/show/CNVD-2021-09907

https://www.cnvd.org.cn/flaw/show/CNVD-2021-09905

https://www.cnvd.org.cn/flaw/show/CNVD-2021-10540

https://www.cnvd.org.cn/flaw/show/CNVD-2021-10541

https://www.cnvd.org.cn/flaw/show/CNVD-2021-10538

2、Cisco 产品安全漏洞

Cisco Smart Software Manager Satellite 是一个为用于提供许可证智能管理功能的软件。Cisco Data Center Network Manager (DCNM)是 Cisco 的一套数据中心网络管理器。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞可通过诱使界面用户点击链接利用该漏洞在受影响的设备上执行任意脚本代码，向受影响的设备发送特制 HTTP 请求利用该漏洞越权编辑配置，发送特制 HTTP 请求利用该漏洞以管理员权限列出、查看、创建、编辑和删除特定系统配置，可通过向受影响设备发送恶意的 HTTP 请求利用该漏洞在底层操作系统上执行任意命令等。

CNVD 收录的相关漏洞包括：Cisco Smart Software Manager Satellite Web UI 命令注入漏洞（CNVD-2021-09935、CNVD-2021-09934、CNVD-2021-09933、CNVD-2021-09937、CNVD-2021-09936）、Cisco Data Center Network Manager 反射型文件下载漏洞、Cisco Data Center Network Manager 授权绕过漏洞（CNVD-2021-09949、CNVD-2021-09948）。其中，“Cisco Smart Software Manager Satellite Web UI 命令注入漏洞（CNVD-2021-09935、CNVD-2021-09934、CNVD-2021-09933、CNVD-2021-09937、CNVD-2021-09936）”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-2021-09935

https://www.cnvd.org.cn/flaw/show/CNVD-2021-09934

https://www.cnvd.org.cn/flaw/show/CNVD-2021-09933

https://www.cnvd.org.cn/flaw/show/CNVD-2021-09937

https://www.cnvd.org.cn/flaw/show/CNVD-2021-09936

https://www.cnvd.org.cn/flaw/show/CNVD-2021-09944

https://www.cnvd.org.cn/flaw/show/CNVD-2021-09949

https://www.cnvd.org.cn/flaw/show/CNVD-2021-09948

3、Adobe 产品安全漏洞

Adobe Photoshop 是美国奥多比（Adobe）公司的一套图片处理软件。Adobe Animate 是美国奥多比（Adobe）公司的一套 Flash 动画制作软件。Adobe Illustrator 是美国奥多比（Adobe）公司的一套基于向量的图像制作软件。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 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，攻击者可利用漏洞执行任意代码。

CNVD 收录的相关漏洞包括：Adobe Photoshop 越界写入漏洞（CNVD-2021-11019）、Adobe Animate 越界写入漏洞、Adobe Illustrator 越界写入漏洞（CNVD-2021-11016、CNVD-2021-11017）、Adobe Photoshop 越界读取漏洞（CNVD-2021-11022）、Adobe Photoshop 缓冲区溢出漏洞（CNVD-2021-11021、CNVD-2021-11020）、多款 Adobe 产品内存错误引用漏洞（CNVD-2021-11024）。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-2021-11019

https://www.cnvd.org.cn/flaw/show/CNVD-2021-11018

https://www.cnvd.org.cn/flaw/show/CNVD-2021-11017

https://www.cnvd.org.cn/flaw/show/CNVD-2021-11016

https://www.cnvd.org.cn/flaw/show/CNVD-2021-11022

https://www.cnvd.org.cn/flaw/show/CNVD-2021-11021

https://www.cnvd.org.cn/flaw/show/CNVD-2021-11020

https://www.cnvd.org.cn/flaw/show/CNVD-2021-11024

4、Microsoft 产品安全漏洞

Microsoft Windows 操作系统是美国微软公司研发的一套操作系统。Microsoft Word 是美国微软（Microsoft）公司的一套 Office 套件中的文字处理软件。Microsoft Windows Server 是一套服务器操作系统。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运行特制应用程序利用该漏洞以提升的权限运行任意代码，运行特制应用程序利用该漏洞提升权限，导致目标主机发生蓝屏等。

CNVD 收录的相关漏洞包括：Microsoft Windows TCP/IP 远程执行代码漏洞、Mic

rosoft Windows TCP/IP 拒绝服务漏洞、Microsoft Windows 和 Windows Server 权限提升漏洞（CNVD-2021-11039、CNVD-2021-11040）、Microsoft Word 远程代码执行漏洞（CNVD-2021-11032、CNVD-2021-11036、CNVD-2021-11035、CNVD-2021-11031）。其中“Microsoft Windows TCP/IP 远程执行代码漏洞、Microsoft Windows TCP/IP 拒绝服务漏洞、Microsoft Word 远程代码执行漏洞（CNVD-2021-11031）、Microsoft Windows 和 Windows Server 权限提升漏洞（CNVD-2021-11039、CNVD-2021-11040）”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-2021-10528
https://www.cnvd.org.cn/flaw/show/CNVD-2021-10529
https://www.cnvd.org.cn/flaw/show/CNVD-2021-11031
https://www.cnvd.org.cn/flaw/show/CNVD-2021-11039
https://www.cnvd.org.cn/flaw/show/CNVD-2021-11040
https://www.cnvd.org.cn/flaw/show/CNVD-2021-11032
https://www.cnvd.org.cn/flaw/show/CNVD-2021-11036
https://www.cnvd.org.cn/flaw/show/CNVD-2021-11035

5、Centreon SQL 注入漏洞（CNVD-2021-11075）

Centreon 是一款免费且开源的 IT 和应用程序监控软件。本周，Centreon 被披露存在 SQL 注入漏洞。攻击者可利用该漏洞注入 SQL 查询，从而可实现远程命令执行。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-2021-11075

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-2021-09932	OpenWrt 释放后重用漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://git.openwrt.org/?p=openwrt/openwrt.git;a=commit;h=5625f5bc36954d644cb80adf8de47854c65d91c3
CNVD-2021-10481	Wordpress wpDataTables SQL 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://wordpress.org/plugins/wpdatatables/#developers
CNVD-2021-10493	Zulip Desktop 远程代码执行漏洞	高	厂商已发布相关漏洞补丁链接，请及时更新：https://blog.zulip.com/2020/04/01/zulip-

			desktop-5-0-0-security-release/
CNVD-2021-11054	Accellion FTA 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://www.accellion.com/products/fta/
CNVD-2021-11055	Accellion FTA 服务器端请求伪造漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://www.accellion.com/products/fta/
CNVD-2021-11053	Accellion FTA OS 命令注入漏洞（CNVD-2021-11053）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.accellion.com/products/fta/
CNVD-2021-11052	Accellion FTA SQL 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://www.accellion.com/products/fta/
CNVD-2021-11064	Micro Focus Operations Bridge Reporter 远程代码执行漏洞	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://softwaresupport.softwaregrp.com/doc/KM03775947
CNVD-2021-11069	Soar Cloud System SQL 注入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：http://www.cge.com.tw/
CNVD-2021-11068	GateManager 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://www.secomea.com/support/cybersecurity-advisory/#2918

小结：本周，Google 产品被披露存在多个漏洞，攻击者可利用漏洞导致需要系统执行特权的权限本地升级，提交特殊的请求，可提升权限，导致拒绝服务等。此外，Cisco、Adobe、Microsoft 等多款产品被披露存在多个漏洞，攻击者可利用漏洞通过诱使界面用户点击链接利用该漏洞在受影响的设备上执行任意脚本代码，通过运行特制应用程序利用该漏洞以提升的权限运行任意代码，运行特制应用程序利用该漏洞提升权限，导致目标主机发生蓝屏等。另外，Centreon 被披露存在 SQL 注入漏洞。攻击者可利用该漏洞注入 SQL 查询，从而可实现远程命令执行。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、Oscar Arzola PressBooks 跨站脚本漏洞

验证描述

Oscar Arzola PressBooks 是中国 Oscar Arzolat 个人开发者的一个应用系统。提供一种图书内容管理系统。。

PressBooks 在 5.17.3 版本中存在跨站脚本漏洞。该漏洞可通过向平台提交长的书本描述来引发存储型 XSS 漏洞。

验证信息

POC 链接：https://www.gosecure.net/blog/2021/02/16/cve-2021-3271-pressbooks-stored-cross-site-scripting-proof-of-concept/

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2021-11067

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. WatchDog 僵尸网络针对加密矿活动中的 Windows 和 Linux 服务器

PaloAlto Network 警告 WatchDog 僵尸网络正在利用来接管 Windows 和 Linux 服务器并挖掘加密货币。

参考链接：https://securityaffairs.co/wordpress/114720/malware/watchdog-botnet.html

2. Cisco Talos 警告说，木马会从 Chromium 浏览器，Outlook 等渠道获取用户登录信息

Cisco Talos 发现了一个凭证窃取木马，该木马可从 Chrome 浏览器，Microsoft 的 Outlook 和即时通讯程序中获取用户登录详细信息。

参考链接：https://www.theregister.com/2021/02/18/masslogger_cisco_talos_research/

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