国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2021 年 03 月 15 日-2021 年 03 月 21 日　　2021 年第 11 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 679 个，其中高危漏洞 120 个、中危漏洞 299 个、低危漏洞 260 个。漏洞平均分值为 4.98。本周收录的漏洞中，涉及 0day 漏洞 427 个（占 63%），其中互联网上出现“CSZ CMS 跨站脚本漏洞（CNVD-2021-19691）、jsPDF 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 4981 个，与上周（4752 个）环比增加 5%。

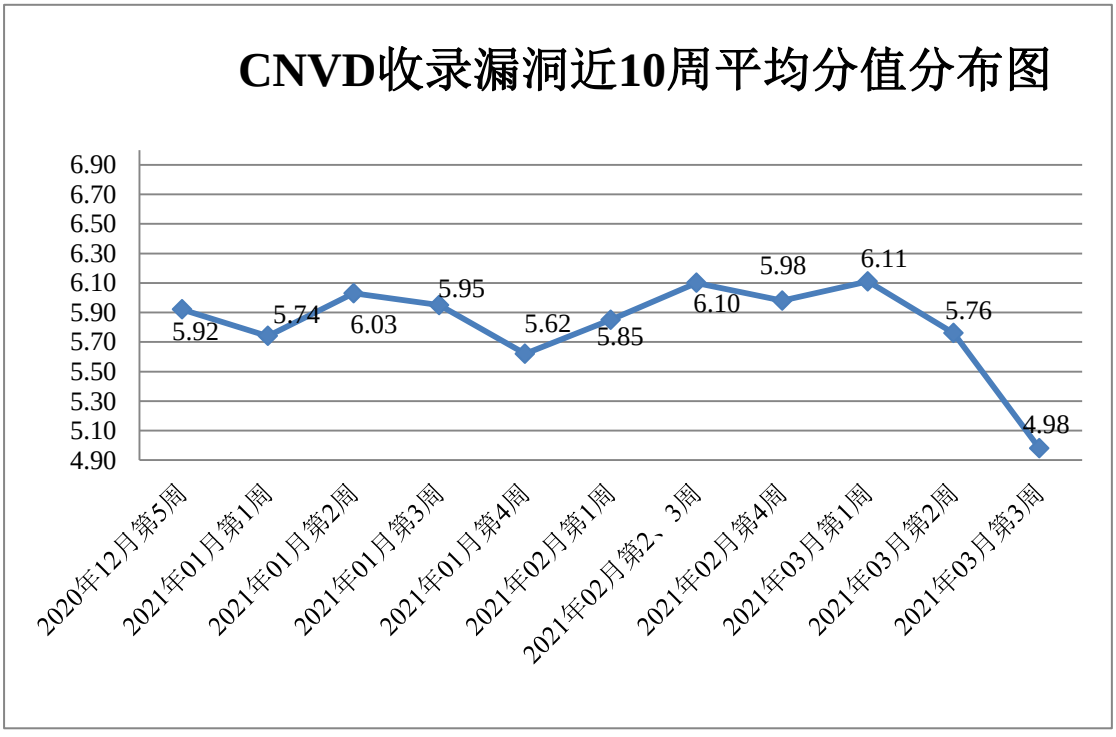

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 21 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 439 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 133 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 35 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：

广东一一五科技股份有限公司、南京九则软件科技有限公司、首岳资讯网络股份有限公司、北京米尔伟业科技有限公司、安信证券股份有限公司、浙江大华技术股份有限公司、网旭科技有限公司、杭州新中大科技股份有限公司、成都飞鱼星科技股份有限公司、畅捷通信息技术股份有限公司、济南驰骋信息技术有限公司、成都俊云科技有限公司、紫光软件系统有限公司、福建福昕软件开发股份有限公司、暴雪娱乐有限公司、北京搜狗信息服务有限公司、润申信息科技（上海）有限公司、成都西维数码科技有限公司、深圳市网旭科技有限公司、广州易神软件科技有限公司、北京火绒网络科技有限公司、天地伟业技术有限公司、北京迪科远望科技有限公司、深圳市明源云科技有限公司、北京升鑫网络科技有限公司、杭州巨峰科技有限公司、海南有趣科技有限公司、万兴科技集团股份有限公司、金通证券有限责任公司、苏州科达科技股份有限公司、广州虎牙信息科技有限公司、联储证券有限责任公司、九州证券股份有限公司、东方财富证券股份有限公司、天风证券股份有限公司、新时代证券股份有限公司、深圳市华德安科技有限公司、民生证券股份有限公司、成都星锐蓝海网络科技有限公司、方正中期期货有限公司、深圳市房多多网络科技有限公司、北京海腾时代科技有限公司、江下信息科技（惠州）有限公司、上海二三四五移动科技有限公司、北京网康科技有限公司、南京铱迅信息技术股份有限公司、廊坊市极致网络科技有限公司、微软(中国)有限公司、北京通达信科科技有限公司、库卡（KUKA）机器人有限公司、浙江同花顺云软件有限公司、东北证券股份有限公司、大通证券股份有限公司、中邮证券有限责任公司、中国中金财富证券有限公司、三星（中国）投资有限公司、海南易而优科技有限公司、太平洋证券股份有限公司、中国中信集团有限公司、世纪证券有限责任公司、上海嵩恒网络科技有限公司、广东熠鑫软件开发有限公司、北京西南偏南科技有限公司、河南青峰网络科技有限公司、华西期货有限责任公司、西南证券股份有限公司、申万宏源证券有限公司、金元证券股份有限公司、中信建投证券股份有限公司、北京猿力教育科技有限公司、咪咕视讯科技有限公司、北京云因信息技术有限公司、北京华夏大地远程教育网络服务有限公司、成都润格无限科技有限公司、上海卓卓网络科技有限公司、校无忧科技网络公司、珠海金山办公软件有限公司、江苏卓顿信息科技有限公司、北京山石网科信息技术有限公司、温州橙树网络技术有限公司、友讯电子设备（上海）有限公司、成都市智蜂网科技有限责任公司、贝尔金国际有限公司、江西铭软科技有限公司、天津速读科技有限公司、北京致远互联软件股份有限公司、苹果电子产品商贸(北京)有限公司、福建智度科

技有限公司、科大讯飞股份有限公司、北京搜狗科技发展有限公司、钉钉（中国）信息技术有限公司、安徽小皮教育科技有限公司、广州津虹网络传媒有限公司、北京世纪长秋科技有限公司、普联技术有限公司、锐捷网络股份有限公司、杭州海康威视数字技术股份有限公司、上海艾泰科技有限公司、微软（中国）有限公司、北京小米科技有限责任公司、深圳市迅雷网络技术有限公司、合肥奇乐网络科技有限公司、安徽省科迅教育装备有限公司、大连大有吴涛易语言软件开发有限公司、上海喜马拉雅科技有限公司、湖北点点点科技有限公司、北京艾科网信科技有限公司、北京爱奇艺科技有限公司、皖新文化科技有限公司、厦门市月轮网络科技有限公司、杭州易玩科技有限公司、《中国学术期刊（光盘版）》电子杂志社有限公司、海南赞赞网络科技有限公司、武汉斗鱼鱼乐网络科技有限公司、灵宝简好网络科技有限公司、上海泛微网络科技股份有限公司、慧星软件科技有限公司、江苏金智教育信息股份有限公司、深圳科士达科技股份有限公司、科立讯通信股份有限公司、长沙市天心区斌网网络技术服务部、北京华御科技有限公司、网易有道信息技术（北京）有限公司、湖南强智科技发展有限公司、北京百度网讯科技有限公司、广东精工智能系统有限公司、金砖通讯科技股份有限公司、襄阳软宝信息科技有限公司、西部动力（北京）科技有限公司、淄博闪灵网络科技有限公司、常州微诺信息科技有限公司、广西集翔网大信息科技有限公司、北京硕人时代科技股份有限公司、深圳市亿图软件有限公司、南京易天智能教育科技有限公司、北京网易有道计算机系统有限公司、北京良精志诚科技有限责任公司、深圳市吉祥腾达科技有限公司、哈尔滨伟成科技有限公司、上海金慧软件有限公司、杭州网易质云科技有限公司、猎豹移动公司、暴风集团股份有限公司、上海硬通网络科技有限公司、网易公司、海通证券股份有限公司、财信证券有限责任公司、财通证券股份有限公司、和利时集团、百度安全应急响应中心、阿里巴巴集团安全应急响应中心、京东安全应急响应中心、雷风影视、优客 365 网址导航、快转视频格式转换器、华夏 ERP、Joomla!、115CMS、鱼跃 CMS、NetSarang、Sumatra PDF、Valve、XUEIDC、JPress、WDJA、ucms、YYCMS、Oracle、Adobe、TOTOLINK、XnView 和 zzzcms。

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，哈尔滨安天科技集团股份有限公司、北京天融信网络安全技术有限公司、新华三技术有限公司、北京神州绿盟科技有限公司、华为技术有限公司等单位报送公开收集的漏洞数量较多。北京华云安信息技术有限公司、杭州海康威视数字技术股份有限公司、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、河南灵创电子科技有限公司 、北京天地和兴科技有限公司、山东新潮信息技术有限公司、武汉明嘉信信息安全检测评估有限公司、贵州多彩宝互联网服务有限公司、河南信安世纪科技有限公司、山东华鲁科技发展股份有限公司、重庆贝特计算机系统工

程有限公司、山东云天安全技术有限公司、杭州迪普科技股份有限公司、北京华顺信安科技有限公司、江苏保旺达软件技术有限公司、杭州木链物联网科技有限公司、新疆海狼科技有限公司、北京安帝科技有限公司、海南神州希望网路有限公司、上海纽盾科技股份有限公司、上海犀点意象网络科技有限公司、安徽长泰信息安全服务有限公司、北方实验室（沈阳）股份有限公司、广州安亿信软件科技有限公司、中国通信服务重庆公司、京东云安全、山石网科通信技术股份有限公司、北京君云天下科技有限公司、山东泽鹿安全技术有限公司、北京山石网科信息技术有限公司、上海观安信息技术股份有限公司、四川哨兵信息科技有限公司、北京惠而特科技有限公司、广西塔易信息技术有限公司、广州市云聚数据服务有限公司、上海崤函信息科技有限公司、神州网安（北京）信息科技有限公司及其他个人白帽子向 CNVD 提交了 4981 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）和斗象科技（漏洞盒子）向 CNVD 共享的白帽子报送的 3526 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
奇安信网神（补天平台）	2363	2363
斗象科技（漏洞盒子）	1163	1163
哈尔滨安天科技集团股份有限公司	300	0
北京天融信网络安全技术有限公司	283	1
新华三技术有限公司	121	0
北京神州绿盟科技有限公司	110	0
华为技术有限公司	84	0
深信服科技股份有限公司	83	3
北京启明星辰信息安全技术有限公司	68	9
中国电信股份有限公司网络安全产品运营中心	54	34
中国电信集团系统集成有限责任公司	44	44
北京数字观星科技有	39	0

限公司		
北京奇虎科技有限公司	27	27
远江盛邦（北京）网络安全科技股份有限公司	20	20
国瑞数码零点实验室	12	12
内蒙古奥创科技有限公司	11	11
北京长亭科技有限公司	9	9
卫士通信息产业股份有限公司	6	0
北京知道创宇信息技术股份有限公司	2	0
北京智游网安科技有限公司	1	1
北京华云安信息技术有限公司	92	92
杭州海康威视数字技术股份有限公司	69	69
北京信联科汇科技有限公司	64	64
南京众智维信息科技有限公司	57	57
河南灵创电子科技有限公司	30	30
北京天地和兴科技有限公司	26	26
山东新潮信息技术有限公司	24	24
武汉明嘉信信息安全检测评估有限公司	22	22
贵州多彩宝互联网服	17	17

务有限公司		
河南信安世纪科技有限公司	17	17
山东华鲁科技发展股份有限公司	16	16
重庆贝特计算机系统工程有限公司	16	16
山东云天安全技术有限公司	14	14
杭州迪普科技股份有限公司	14	0
北京华顺信安科技有限公司	13	0
江苏保旺达软件技术有限公司	10	10
杭州木链物联网科技有限公司	10	10
新疆海狼科技有限公司	10	10
北京安帝科技有限公司	8	8
海南神州希望网路有限公司	8	8
上海纽盾科技股份有限公司	8	8
上海犀点意象网络科技有限公司	8	8
安徽长泰信息安全服务有限公司	6	6
北方实验室（沈阳）股份有限公司	5	5
广州安亿信软件科技有限公司	5	5
中国通信服务重庆公	4	4

司		
京东云安全	4	4
山石网科通信技术股份有限公司	4	4
北京君云天下科技有限公司	3	3
山东泽鹿安全技术有限公司	3	3
北京山石网科信息技术有限公司	2	2
上海观安信息技术股份有限公司	2	2
四川哨兵信息科技有限公司	2	2
北京惠而特科技有限公司	1	1
广西塔易信息技术有限公司	1	1
广州市云聚数据服务有限公司	1	1
上海崤函信息科技有限公司	1	1
神州网安（北京）信息科技有限公司	1	1
CNCERT 宁夏分中心	9	9
CNCERT 西藏分中心	2	2
CNCERT 河北分中心	1	1
个人	701	701
报送总计	6111	4981

本周漏洞按类型和厂商统计

本周，CNVD 收录了 679 个漏洞。应用程序 417 个，WEB 应用 141 个，网络设备（交换机、路由器等网络端设备）66 个，安全产品 8 个，操作系统 34 个，智能设备（物联网终端设备）13 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	417
WEB 应用	141
网络设备（交换机、路由器等网络端设备）	66
操作系统	34
智能设备（物联网终端设备）	13
安全产品	8

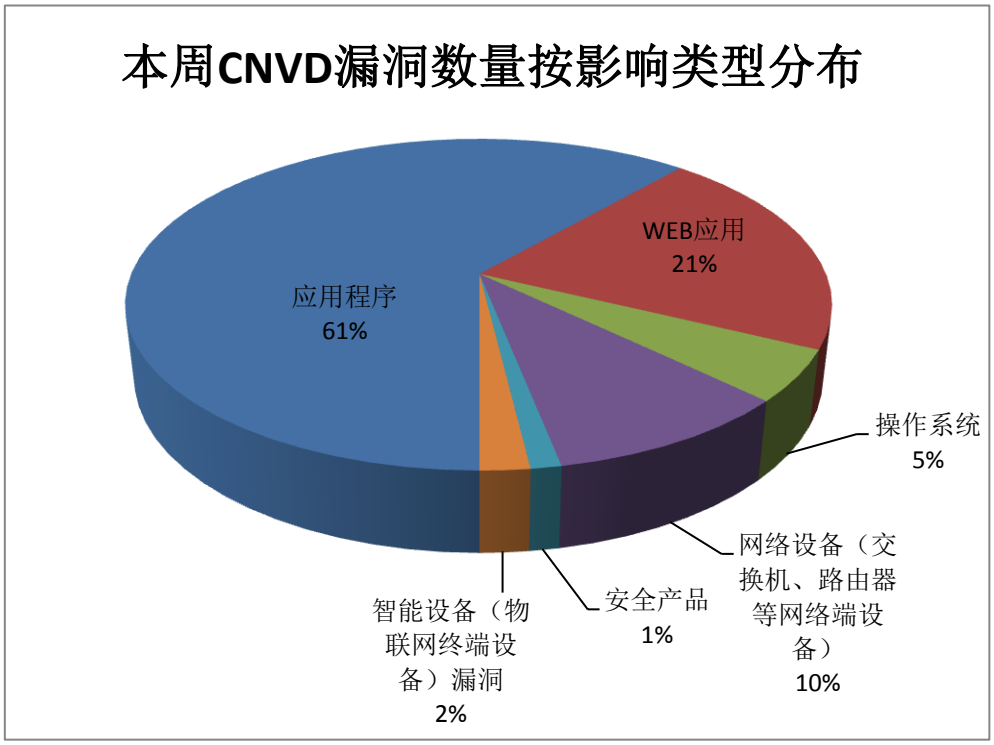

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Google、广州虎牙信息科技有限公司、深圳市腾讯计算机系统有限公司等多家厂商的产品，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	Google	29	4%
2	广州虎牙信息科技有限公司	19	3%
3	深圳市腾讯计算机系统有限公司	19	3%
4	Adobe	17	2%
5	GitLab	14	2%
6	Linux	13	2%
7	NETGEAR	13	2%

8	Red Hat	13	2%
9	锐捷网络股份有限公司	13	2%
10	其他	529	78%

本周行业漏洞收录情况

本周，CNVD 收录了 47 个电信行业漏洞，48 个移动互联网行业漏洞，30 个工控行业漏洞（如下图所示）。其中，“D-Link DIR-841 命令注入漏洞、NETGEAR JGS516PE/GS116Ev2 固件更新漏洞、NETGEAR JGS516PE/GS116Ev2 任意数据写入漏洞、Schneider Electric Interactive Graphical SCADA System 缓冲区溢出漏洞（CNVD-2021-18389）”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/

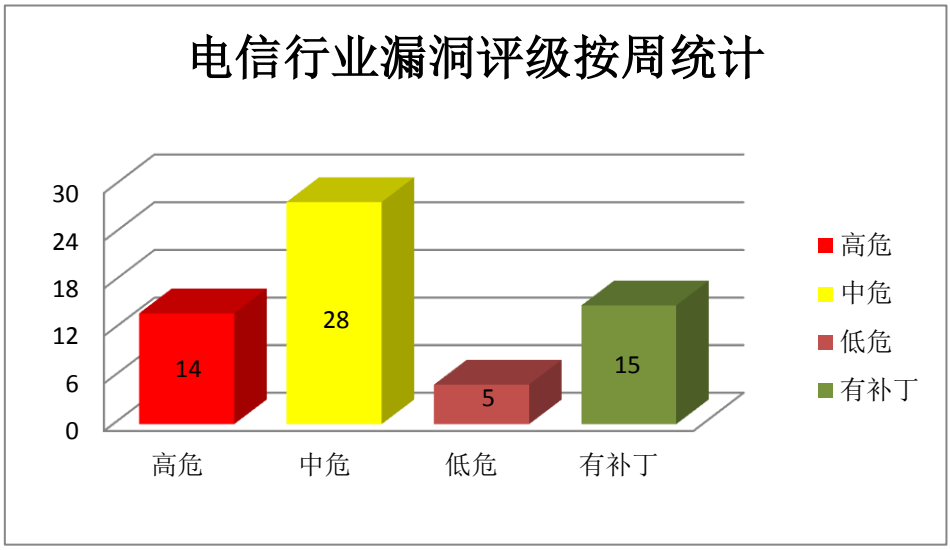

图 3 电信行业漏洞统计

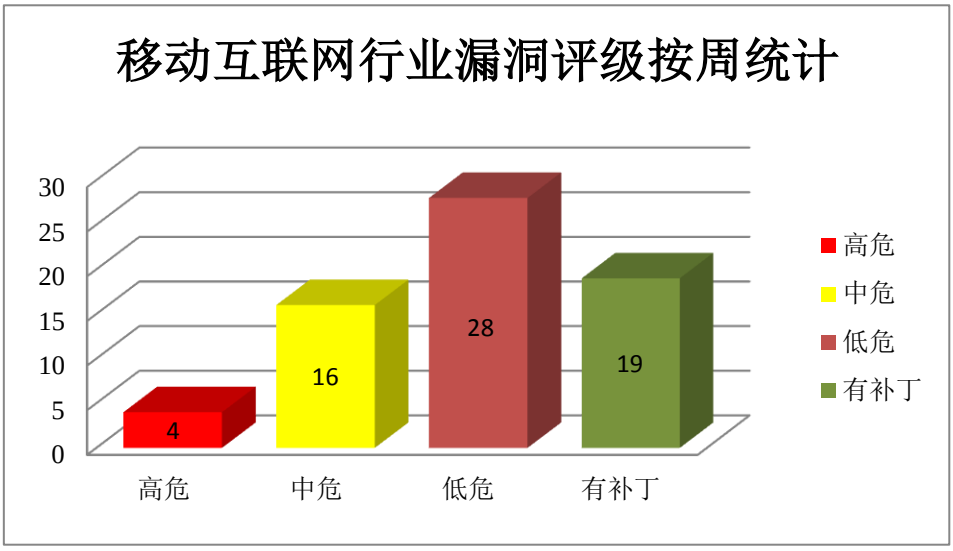

图 4 移动互联网行业漏洞统计

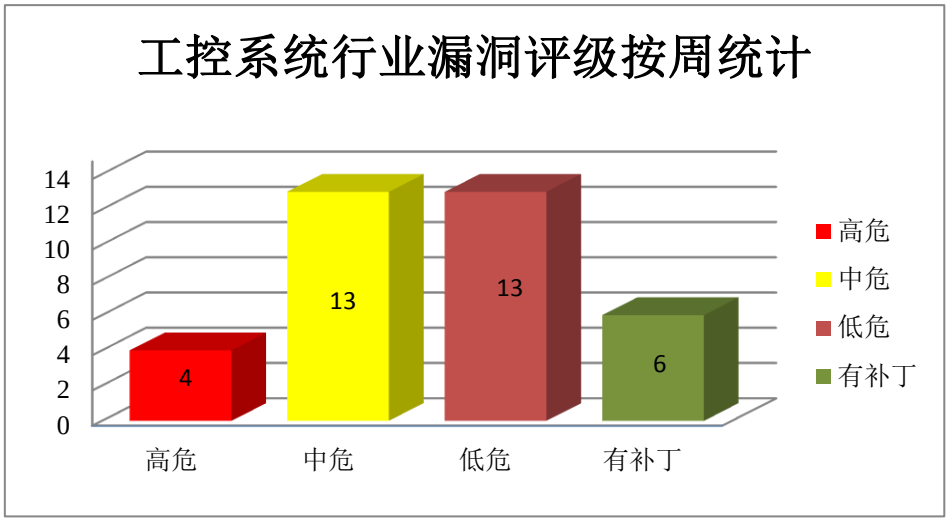

图 5 工控系统行业漏洞统计

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、 Google 产品安全漏洞

Chrome 是由 Google 开发的一款设计简单、高效的 Web 浏览工具，其特点是简洁、快速。Android 是美国 Google 公司和开放手持设备联盟（简称 OHA）共同开发的一套以 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，攻击者可利用漏洞通过精心制作的 HTML 页面从进程内存中获取潜在的敏感信息，导致特权的本地升级，而无需其他执行特权，实现远程代码执行等。

CNVD 收录的相关漏洞包括：Google Chrome 策略执行不足漏洞（CNVD-2021-17299）、Google Chrome 安全性 UI 不正确漏洞（CNVD-2021-17298）、Google Chrome 释

放后重用漏洞（CNVD-2021-17300）、Google Android System 远程代码执行漏洞（CNVD-2021-17303）、Google Android System 权限提升漏洞（CNVD-2021-17302）、Google Android System 远程代码执行漏洞（CNVD-2021-17304）、Google Android Framework 权限提升漏洞（CNVD-2021-17306）。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-2021-17299
https://www.cnvd.org.cn/flaw/show/CNVD-2021-17298
https://www.cnvd.org.cn/flaw/show/CNVD-2021-17300
https://www.cnvd.org.cn/flaw/show/CNVD-2021-17303
https://www.cnvd.org.cn/flaw/show/CNVD-2021-17302
https://www.cnvd.org.cn/flaw/show/CNVD-2021-17304
https://www.cnvd.org.cn/flaw/show/CNVD-2021-17306
https://www.cnvd.org.cn/flaw/show/CNVD-2021-17305

2、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。该软件主要用于处理图片。Adobe FrameMaker 是一款文档处理程序，用于编写和编辑包括结构化文档在内的大型或复杂文档。Adobe Connect 是一款在线视频会议软件。Adobe Animate 是美国奥多比（Adobe）公司的一套 Flash 动画制作软件。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞借助恶意文件利用该漏洞导致信息泄露，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-2021-17735）、Adobe Framemaker 越界读取漏洞（CNVD-2021-17742）、Adobe Connect 输入验证不当漏洞、Adobe Animate 越界读取漏洞（CNVD-2021-17737、CNVD-2021-17736、CNVD-2021-17740、CNVD-2021-17739）、Adobe Animate 内存破坏漏洞（CNVD-2021-17741）。其中“Adobe Photoshop 越界写入漏洞（CNVD-2021-17735）、Adobe Framemaker 越界读取漏洞（CNVD-2021-17742）、Adobe Connect 输入验证不当漏洞”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-2021-17735
https://www.cnvd.org.cn/flaw/show/CNVD-2021-17742
https://www.cnvd.org.cn/flaw/show/CNVD-2021-18027
https://www.cnvd.org.cn/flaw/show/CNVD-2021-17737
https://www.cnvd.org.cn/flaw/show/CNVD-2021-17736
https://www.cnvd.org.cn/flaw/show/CNVD-2021-17741
https://www.cnvd.org.cn/flaw/show/CNVD-2021-17740
https://www.cnvd.org.cn/flaw/show/CNVD-2021-17739

3、SAP 产品安全漏洞

SAP Enterprise Financial Services 是德国思爱普（SAP）公司的一套企业财务服务解决方案。SAP NetWeaver Knowledge Management Configuration Service 是德国思爱普（SAP）公司的一款知识管理解决方案配置服务。SAP HANA 是德国思爱普（SAP）公司的一套高性能的实时数据分析平台。SAP MII 是德国思爱普（SAP）公司的一个应用软件。SAP Netweaver 是德国思爱普（SAP）公司的一套面向服务的集成化应用平台。SAP Netweaver Application Server Java 是 SAP NetWeaver Application Platform 的一部分，其提供用于部署和运行 Java 应用程序的完整基础架构。SAP Business Warehouse（BW）是 SAP 的数据仓库解决方案。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞将用户重定向到恶意站点，提升权限，通过远程启用功能模块利用该漏洞注入代码等。

CNVD 收录的相关漏洞包括：SAP Enterprise Financial Services 权限提升漏洞（CNVD-2021-18017）、SAP NetWeaver Knowledge Management Configuration Service 不安全反序列化漏洞、SAP HANA 身份验证绕过漏洞（CNVD-2021-18021）、SAP MII 代码注入漏洞、SAP NetWeaver 未授权访问漏洞、SAP Netweaver Application Server Java 反向标签钓鱼漏洞、SAP AS ABAP 和 SAP S4 HANA 身份验证不当漏洞、SAP Business Warehouse 和 SAP BW/4HANA 代码注入漏洞。其中“SAP HANA 身份验证绕过漏洞（CNVD-2021-18021）、SAP MII 代码注入漏洞、SAP NetWeaver 未授权访问漏洞、SAP AS ABAP 和 SAP S4 HANA 身份验证不当漏洞”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-2021-18017
https://www.cnvd.org.cn/flaw/show/CNVD-2021-18016
https://www.cnvd.org.cn/flaw/show/CNVD-2021-18021
https://www.cnvd.org.cn/flaw/show/CNVD-2021-18019
https://www.cnvd.org.cn/flaw/show/CNVD-2021-18020
https://www.cnvd.org.cn/flaw/show/CNVD-2021-18018
https://www.cnvd.org.cn/flaw/show/CNVD-2021-18229
https://www.cnvd.org.cn/flaw/show/CNVD-2021-18228

4、Red Hat 产品安全漏洞

Red Hat Enterprise Linux 是美国红帽（Red Hat）公司的面向企业用户的 Linux 操作系统。Red Hat Undertow 是美国红帽（Red Hat）公司的一款基于 Java 的嵌入式 Web 服务器，是 Wildfly（Java 应用服务器）默认的 Web 服务器。Red Hat Wildfly 是美国红帽（Red Hat）公司的一款基于 JavaEE 的轻量级开源应用服务器。Red Hat Keycloak 是美国红帽（Red Hat）公司的一套为现代应用和服务提供身份验证和管理功能的软件。

Red Hat Hibernate ORM 是美国红帽（Red Hat）公司的一款用于编写应用程序的对象/关系映射（ORM）框架。JPA Criteria API 是其中的一个用于查询功能的 API（应用程序编程接口）。Red Hat Satellite 是美国红帽（Red Hat）公司的一套系统管理平台。Red Hat 3scale API Management Platform 是美国红帽（Red Hat）公司的一个 API 管理的基础架构平台。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞导致缓冲区溢出或堆溢出，通过特殊字符查询触发致命错误，以触发拒绝服务，访问未授权的信息或进行进一步的攻击等。

CNVD 收录的相关漏洞包括：Red Hat Enterprise Linux 资源管理错误漏洞（CNVD-2021-19382）、Red Hat Undertow 拒绝服务漏洞、Red Hat Wildfly 内存泄露漏洞、Red Hat Keycloak 跨站脚本漏洞（CNVD-2021-17784）、Red Hat Hibernate ORM SQL 注入漏洞、Red Hat Satellite 缓冲区溢出漏洞、Red Hat 3scale API Management Platform 输入验证错误漏洞、Red Hat Keycloak 访问控制错误漏洞（CNVD-2021-19376）。其中“Red Hat Enterprise Linux 资源管理错误漏洞（CNVD-2021-19382）、Red Hat Undertow 拒绝服务漏洞、Red Hat Wildfly 内存泄露漏洞”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-2021-19382
https://www.cnvd.org.cn/flaw/show/CNVD-2021-19380
https://www.cnvd.org.cn/flaw/show/CNVD-2021-19385
https://www.cnvd.org.cn/flaw/show/CNVD-2021-17784
https://www.cnvd.org.cn/flaw/show/CNVD-2021-18234
https://www.cnvd.org.cn/flaw/show/CNVD-2021-19378
https://www.cnvd.org.cn/flaw/show/CNVD-2021-19377
https://www.cnvd.org.cn/flaw/show/CNVD-2021-19376

5、zzzphp SQL 注入漏洞

zzzphp 是免费开源的建站系统，主要面对广大站长使用,不需要授权,可免费商用。本周，zzzphp 被披露存在 SQL 注入漏洞。攻击者可利用该漏洞执行非法 SQL 命令。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-2021-18394

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-2021-17572	NETGEAR JGS516PE/GS116Ev2 固件更新漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：

			https://www.netgear.com/support/product/GS116Ev2.aspx
CNVD-2021-17729	Microsoft Azure Sphere 权限提升漏洞（CNVD-2021-17729）	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-2020-16992
CNVD-2021-17728	Aviatrix Controller 任意文件上传漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.criticalstart.com/multiple-vulnerabilities-discovered-in-aviatrix/
CNVD-2021-17735	Adobe Photoshop 越界写入漏洞（CNVD-2021-17735）	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/photoshop/apsb21-17.html
CNVD-2021-17742	Adobe Framemaker 越界读取漏洞（CNVD-2021-17742）	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/framemaker/apsb21-14.html
CNVD-2021-17748	Microsoft Defender 远程代码执行漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1647
CNVD-2021-18035	HPE Pay 路径遍历漏洞（CNVD-2021-18035	高	厂商已发布了漏洞修复程序，请及时关注更新：https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=emr_na-hpesbgn04037en_us
CNVD-2021-18037	RIOT 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/RIOT-OS/RIOT/pull/14400/commits/f8ac003bbfe11956578dd2189827686c27374d06
CNVD-2021-18263	MediaTek cameraisp 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://corp.mediatek.com/product-security-acknowledgements
CNVD-2021-18370	SaltStack Salt 代码注入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://repo.saltstack.com

小结：本周，Google 产品被披露存在多个漏洞，攻击者可利用漏洞通过精心制作的 HTML 页面从进程内存中获取潜在的敏感信息，导致特权的本地升级，而无需其他执行特权，实现远程代码执行等。此外，Adobe、SAP、Red Hat 等多款产品被披露存在多个

漏洞，攻击者可利用漏洞导致信息泄露，执行任意代码，导致缓冲区溢出或堆溢出，通过特殊字符查询触发致命错误，以触发拒绝服务等。另外，Seo Panel 被披露存在跨站脚本漏洞。攻击者可通过 archive.php search_name 参数利用该漏洞注入 JavaScript。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、jsPDF 跨站脚本漏洞

验证描述

jsPDF 是一款基于 JavaScript 的 PDF 文档生成库。

jsPDF 所有版本中存在跨站脚本漏洞。该漏洞源于 WEB 应用缺少对客户端数据的正确验证。攻击者可利用该漏洞执行客户端代码。

验证信息

POC 链接：https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARS-575255

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2021-18232

信息提供者

恒安嘉新(北京)科技股份公司

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. 微软的 Azure SDK 网站可以被混入伪造的测试包

一名安全研究人发现能够在微软 Azure SDK 最新版本的官方列表中添加一个假冒的测试包。这个简单的技巧如果被攻击者滥用，就会让人觉得他们的恶意包是 Azure SDK 套件的一部分。

参考链接：https://www.bleepingcomputer.com/news/security/microsofts-azure-sdk-site-tricked-into-listing-fake-package/

2. 攻击者利用 Microsoft Exchange 漏洞攻击智利银行监管机构

智利的墨西哥金融市场委员会（CMF）披露，其 Microsoft Exchange 服务器已因最近披露的 ProxyLogon 漏洞而受到威胁。

参考链接：https://www.bleepingcomputer.com/news/security/chiles-bank-regulator-shares-iocs-after-microsoft-exchange-hack/

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