国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2021 年 01 月 04 日-2021 年 01 月 10 日　　2021 年第 1 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 268，其中高危漏洞 90 个、中危漏洞 140 个、低危漏洞 38 个。漏洞平均分值为 5.74。本周收录的漏洞中，涉及 0day 漏洞 136 个（占 51%），其中互联网上出现“Egavilan Media Under Onstruction Page With Cpanel SQL 注入漏洞、Online Marriage Registration System SQL 注入漏洞”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 3992 个，与上周（6932 个）环比减少 42%。

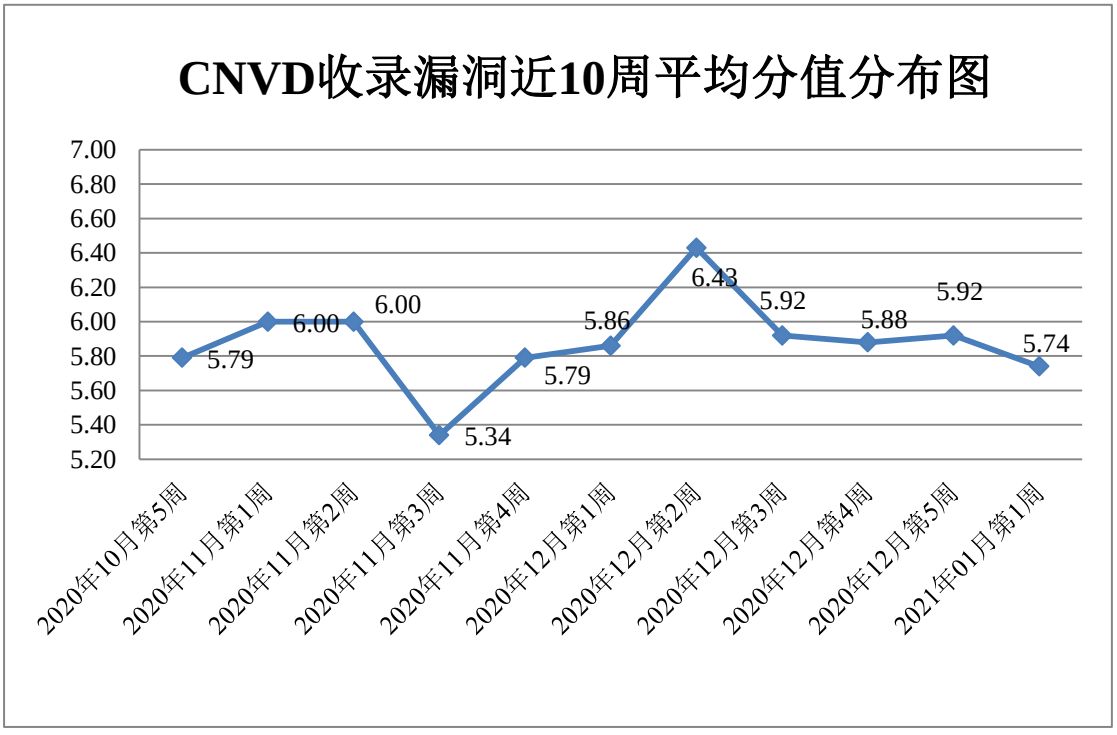

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 10 起，向基础电信企业通报漏洞事件 16 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 234 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 21 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 34 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：

重庆天知软件技术有限公司、厦门狮子鱼网络科技有限公司、江西惠当家信息技术股份有限公司、大唐电信科技股份有限公司、上海锐格软件有限公司、深圳科士达科技股份有限公司、微软(中国)有限公司、正方软件股份有限公司、长沙米拓信息技术有限公司、安徽阳光心健科技发展有限公司、青岛易软天创网络科技有限公司、武汉木仓科技股份有限公司、广州网天网络科技有限公司、北京坤豆科技有限公司、北京爱奇艺科技有限公司、成都康菲顿特网络科技有限公司、北京致远互联软件股份有限公司、深圳市爱思软件技术有限公司、北京因酷时代科技有限公司、深圳市吉祥腾达科技有限公司、美国网件公司、睿谷信息科技有限公司、浙江兰德纵横网络技术股份有限公司、浪潮集团有限公司、深圳市迅雷网络技术有限公司、北京金山办公软件股份有限公司、上海商派网络科技有限公司、浙江宇视科技有限公司、浙江大华技术股份有限公司、河南快鸟软件科技有限公司、北京海腾时代科技有限公司、广州易全信息科技有限公司、重庆本易软件有限公司 、腾智信息技术有限公司、北京飞书科技有限公司、天信仪表集团有限公司、浙江大华技术股份有限公司、广州添富信息科技有限责任公司、北京通达信科科技有限公司、珠海金山办公软件有限公司、南京国图信息产业有限公司、深圳市迪元素科技有限公司、南京冠邦网络技术有限责任公司、鹏为软件股份有限公司、山西企凝信息科技有限公司、青岛易企天创管理咨询有限公司、湖北淘码千维信息科技有限公司、帆软软件有限公司、北京京企科技股份有限公司、深圳市咫尺网络科技开发有限公司、深圳市信锐网科技术有限公司、北京辰信领创信息技术有限公司、上海银狐信息科技有限公司、武汉斗鱼网络科技有限公司、北京行圆汽车信息技术有限公司、北京猎鹰安全科技有限公司、上海新朋程数据科技发展有限公司、北京费尔之盾科技有限公司、北京神奇像素科技有限公司、北京百度网讯科技有限公司、河南青峰网络科技有限公司、上海北辰软件股份有限公司、广州亚美信息科技有限公司、深圳市任想科技有限公司、思科系统（中国）网络技术有限公司、和利时集团、信呼、若依、轻舟云平台 Pro、熊海 CMS、帝云 CMS 、SeaCMS、Citrix Systems, Inc.、HEYBBS、ZZCMS、MikroTik 和 The Apache Software Foundation。

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、哈尔滨安天

科技集团股份有限公司、北京神州绿盟科技有限公司、华为技术有限公司、深信服科技股份有限公司等单位报送公开收集的漏洞数量较多。北京山石网科信息技术有限公司、南京众智维信息科技有限公司、北京天地和兴科技有限公司、国瑞数码零点实验室、河南灵创电子科技有限公司 、上海犀点意象网络科技有限公司、河南信安世纪科技有限公司、杭州迪普科技股份有限公司、山东华鲁科技发展股份有限公司、西安交大捷普网络科技有限公司、北京华云安信息技术有限公司、远江盛邦（北京）网络安全科技股份有限公司、广州市蓝爵计算机科技有限公司、郑州云智信安安全技术有限公司、北京零零信安科技有限公司、江苏保旺达软件技术有限公司、上海观安信息技术股份有限公司、北京网御星云信息技术有限公司、百度 AIoT 安全团队、北京惠而特科技有限公司、安徽长泰信息安全服务有限公司、广州安亿信软件科技有限公司、山东云天安全技术有限公司、新疆海狼科技有限公司、北京时代新威信息技术有限公司、北京云科安信科技有限公司（Seraph 安全实验室）、北京长亭科技有限公司、广西等保安全测评有限公司、国网山东省电力公司、上海纽盾科技股份有限公司、深圳市魔方安全科技有限公司、信联科技（南京）有限公司、北京华顺信安科技有限公司、任子行网络技术股份有限公司、北京机沃科技有限公司、北京智游网安科技有限公司、北京禹宏信安科技有限公司、广西塔易信息技术有限公司、上海市信息安全测评认证中心及其他个人白帽子向 CNVD 提交了 3992 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 2595 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）	1743	1743
奇安信网神（补天平台）	513	513
上海交大	339	339
北京天融信网络安全技术有限公司	297	0
哈尔滨安天科技集团股份有限公司	290	0
北京神州绿盟科技有限公司	213	39
华为技术有限公司	132	0
深信服科技股份有限公司	87	0
北京启明星辰信息安全技术有限公司	86	35
新华三技术有限公司	81	0
北京数字观星科技有限公司	58	0
中国电信股份有限公司网络安全产品运营中心	20	0
中国电信集团系统集成有限责任公司	13	13
北京知道创宇信息技术股份	4	1

有限公司		
杭州安恒信息技术股份有限公司	3	3
北京山石网科信息技术有限公司	97	97
南京众智维信息科技有限公司	93	93
北京天地和兴科技有限公司	44	44
国瑞数码零点实验室	39	39
河南灵创电子科技有限公司	32	32
上海犀点意象网络科技有限公司	17	17
河南信安世纪科技有限公司	16	16
杭州迪普科技股份有限公司	16	0
山东华鲁科技发展股份有限公司	15	15
西安交大捷普网络科技有限公司	13	13
北京华云安信息技术有限公司	12	12
远江盛邦（北京）网络安全科技股份有限公司	12	12
广州市蓝爵计算机科技有限公司	8	8
郑州云智信安安全技术有限公司	8	8
北京零零信安科技有限公司	7	7
江苏保旺达软件技术有限公司	7	7
上海观安信息技术股份有限公司	7	7
北京网御星云信息技术有限公司	6	6
百度 AIoT 安全团队	5	5
北京惠而特科技有限公司	4	4
安徽长泰信息安全服务有限公司	3	3
广州安亿信软件科技有限公司	3	3
山东云天安全技术有限公司	3	3
新疆海狼科技有限公司	3	3
北京时代新威信息技术有限公司	2	2

北京云科安信科技有限公司（Seraph 安全实验室）	2	2
北京长亭科技有限公司	2	2
广西等保安全测评有限公司	2	2
国网山东省电力公司	2	2
上海纽盾科技股份有限公司	2	2
深圳市魔方安全科技有限公司	2	2
信联科技（南京）有限公司	2	2
北京华顺信安科技有限公司	1	1
任子行网络技术股份有限公司	1	1
北京机沃科技有限公司	1	1
北京智游网安科技有限公司	1	1
北京禹宏信安科技有限公司	1	1
广西塔易信息技术有限公司	1	1
上海市信息安全测评认证中心	1	1
CNCERT 贵州分中心	6	6
CNCERT 青海分中心	3	3
CNCERT 四川分中心	3	3
CNCERT 西藏分中心	1	1
个人	816	816
报送总计	5201	3992

本周漏洞按类型和厂商统计

本周，CNVD 收录了 268 个漏洞。应用程序 134 个，WEB 应用 74 个，操作系统 35 个，网络设备（交换机、路由器等网络端设备）9 个，数据库 9 个，安全产品 4 个，智能设备（物联网终端设备）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
应用程序	134
WEB 应用	74
操作系统	35
网络设备（交换机、路由器等网络端设备）	9
数据库	9
安全产品	4
智能设备（物联网终端设备）	3

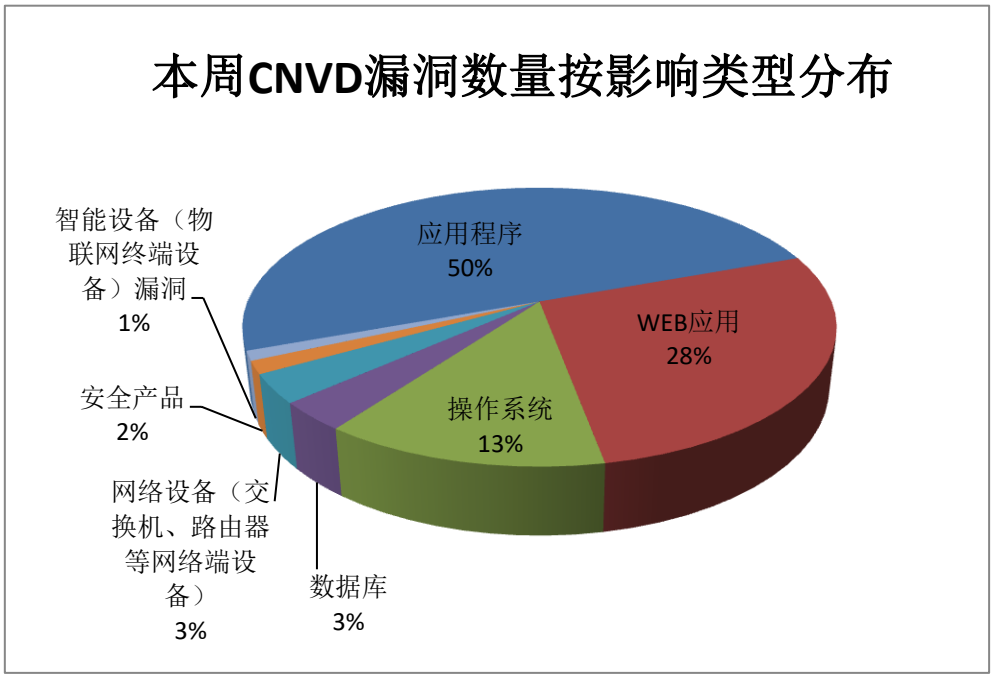

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Google、IBM、Oracle 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	27	10%
2	IBM	14	5%
3	Oracle	12	4%
4	gogogate	10	4%
5	Microsoft	10	4%
6	珠海金山办公软件有限公司	10	4%
7	深圳市汇川技术股份有限公司	9	3%
8	FasterXML	8	3%
9	GNU	8	3%
10	其他	160	60%

本周行业漏洞收录情况

本周，CNVD 收录了 10 个电信行业漏洞，32 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，“Google Android 存在缓冲区溢出漏洞、Google Android Pixel 存在缓冲区溢出漏洞”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/

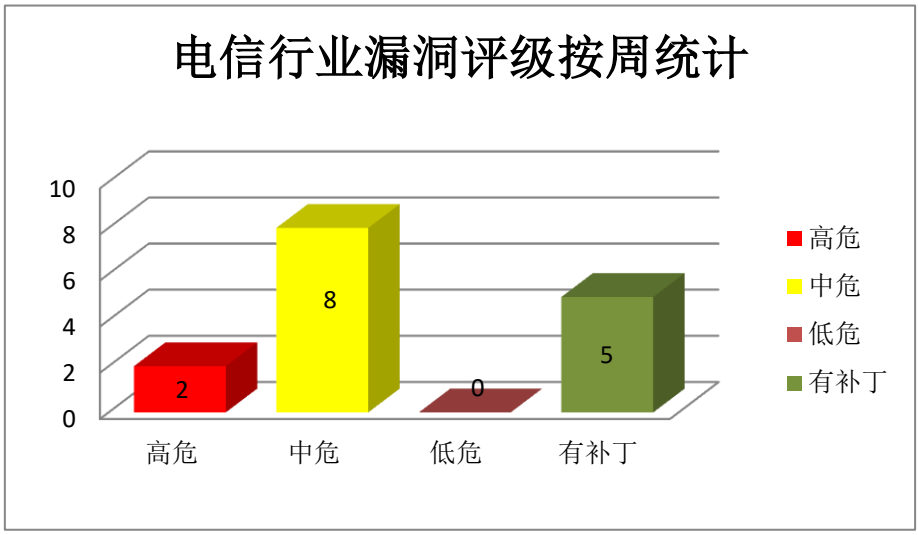

图 3 电信行业漏洞统计

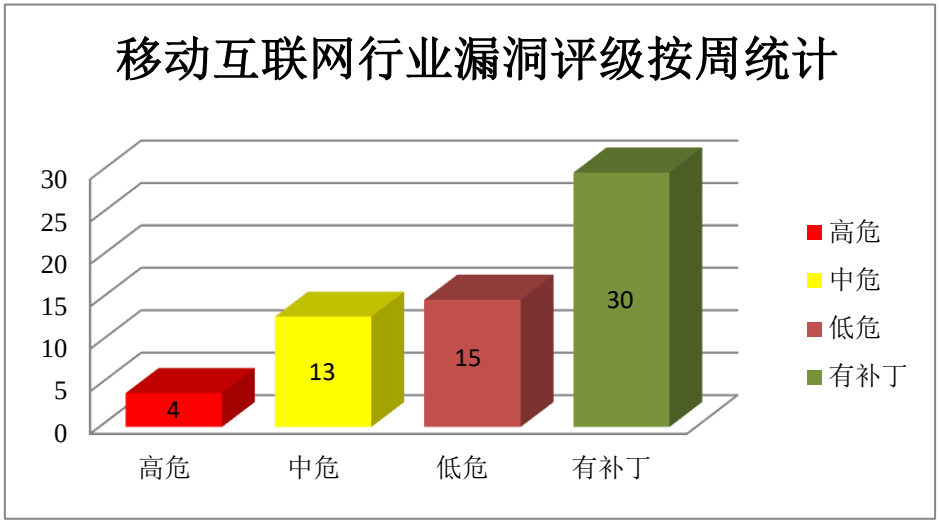

图 4 移动互联网行业漏洞统计

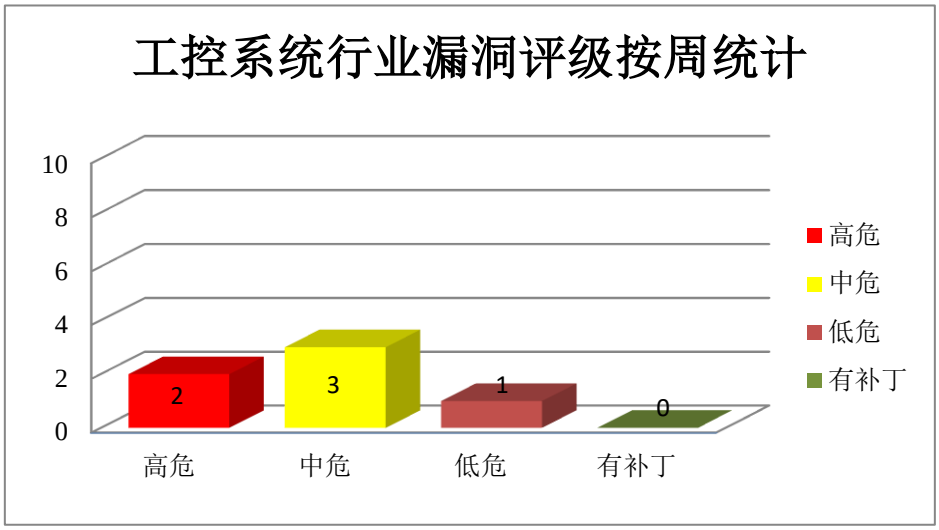

图 5 工控系统行业漏洞统计

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、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所需的系统执行特权在本地升级，导致特权的本地升级，而无需其他执行特权等。

CNVD 收录的相关漏洞包括：Google Android Pixel 本地权限提升漏洞（CNVD-2021-01333、CNVD-2021-01334、CNVD-2021-01335）、Google Android 本地权限提升漏洞（CNVD-2021-01336）、Google Android 拒绝服务漏洞（CNVD-2021-01328、CNVD-2021-01332）、Google Android 权限提升漏洞（CNVD-2021-01329、CNVD-2021-01339）。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-2021-01335

https://www.cnvd.org.cn/flaw/show/CNVD-2021-01333

https://www.cnvd.org.cn/flaw/show/CNVD-2021-01334

https://www.cnvd.org.cn/flaw/show/CNVD-2021-01336

https://www.cnvd.org.cn/flaw/show/CNVD-2021-01328

https://www.cnvd.org.cn/flaw/show/CNVD-2021-01332

https://www.cnvd.org.cn/flaw/show/CNVD-2021-01329

https://www.cnvd.org.cn/flaw/show/CNVD-2021-01339

2、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 Server 是一套服务器操作系统。Windows COM 是美国 Microsoft 公司的一套软件组件的二进制接口标准。该组件使得能够与 Windows 服务进行实时交互。Microsoft Excel 是美国微软（Microsoft）公司的一款 Office 套件中的电子表格处理软件。Microsoft Exchange Server 是 Microsoft 开发的邮件服务器和日历服务器。Microsoft Windows 是美国微软（Microsoft）公司的一套个人设备使用的操作系统。DirectX 是其中的一个多媒体系统链接库。Microsoft Visual Studio 是一个集成的开发环境，用于开发计算机程序、网站、Web 应用程序、Web 服务和移动应用程序。Windows Graphics Device Interface 是美国 Microsoft 公司的一个图形设备接口函数。该函数负责系统与绘图程序之间的信息交换，处理所有 Windows 程序的图形输出。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞在目标系统上执行任意代码，控制受影响的系统，可以安装程序；查看、更改或删除数据；或者创建拥有完全用户权限的新帐户等。

CNVD 收录的相关漏洞包括：Microsoft COM for Windows 远程代码执行漏洞（CNVD-2021-01045）、Microsoft Excel 远程代码执行漏洞（CNVD-2021-01037）、Microsoft Exchange Server 远程代码执行漏洞（CNVD-2021-01044）、Microsoft Microsoft Windows Codecs Library 远程代码执行漏洞（CNVD-2021-01042、CNVD-2021-01043）、Microsoft Visual Studio 远程代码执行漏洞（CNVD-2021-01041）、Microsoft Windows Graphics Device Interface (GDI)远程代码执行漏洞、Microsoft Windows Storage Services 权限提升漏洞。其中，“Microsoft Visual Studio 远程代码执行漏洞（CNVD-2021-01041）、Microsoft Microsoft Windows Codecs Library 远程代码执行漏洞、Microsoft Exchange Server 远程代码执行漏洞（CNVD-2021-01044）、Microsoft COM for Windows 远程代码执行漏洞（CNVD-2021-01045）、Microsoft Windows Graphics Device Interface (GDI) 远程代码执行漏洞”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-2021-01045
https://www.cnvd.org.cn/flaw/show/CNVD-2021-01037
https://www.cnvd.org.cn/flaw/show/CNVD-2021-01044
https://www.cnvd.org.cn/flaw/show/CNVD-2021-01042
https://www.cnvd.org.cn/flaw/show/CNVD-2021-01043
https://www.cnvd.org.cn/flaw/show/CNVD-2021-01041
https://www.cnvd.org.cn/flaw/show/CNVD-2021-01046
https://www.cnvd.org.cn/flaw/show/CNVD-2021-01040

3、IBM 产品安全漏洞

IBM API Connect（APIConnect）是美国 IBM 公司的一套用于管理 API 生命周期的集成解决方案。该产品支持创建、运行、管理和保护 API 和微服务等。IBM Cloud Pak System 是美国 IBM 公司的一套具有可配置、预集成软件的全栈、融合基础架构。IBM

Curam Social Program Management 是美国 IBM 公司的一套社会计划管理解决方案，支持端到端社会项目交付流程。IBM Maximo Asset Management 是美国 IBM 公司的一套综合性资产生命周期和维护管理解决方案。IBM Spectrum Protect Plus 是一套数据保护平台。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞通过纯文本传输绕过对数据的访问限制，以获取敏感信息，执行从网站信任的用户传输的恶意和未经授权的操作，在服务器上执行任意代码等。

CNVD 收录的相关漏洞包括：IBM API Connect 访问控制错误漏洞（CNVD-2021-01274）、IBM Cloud Pak System 会话固定漏洞、IBM Cloud Pak System 跨站请求伪造漏洞（CNVD-2021-01065）、IBM Cloud Pak System 权限提升漏洞、IBM Cloud Pak System 任意文件上传漏洞（CNVD-2021-01067）、IBM Curam Social Program Management 跨站请求伪造漏洞（CNVD-2021-01275）、IBM Maximo Asset Management 跨站请求伪造漏洞（CNVD-2021-01278）、IBM Spectrum Protect Plus 目录遍历漏洞。其中，“IBM API Connect 访问控制错误漏洞（CNVD-2021-01274）”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-2021-01274
https://www.cnvd.org.cn/flaw/show/CNVD-2021-01066
https://www.cnvd.org.cn/flaw/show/CNVD-2021-01065
https://www.cnvd.org.cn/flaw/show/CNVD-2021-01063
https://www.cnvd.org.cn/flaw/show/CNVD-2021-01067
https://www.cnvd.org.cn/flaw/show/CNVD-2021-01275
https://www.cnvd.org.cn/flaw/show/CNVD-2021-01278
https://www.cnvd.org.cn/flaw/show/CNVD-2021-01277

4、Oracle 产品安全漏洞

Oracle Database Server 是美国甲骨文（Oracle）公司的一套关系数据库管理系统。该数据库管理系统提供数据管理、分布式处理等功能。Oracle MySQL Cluster 是美国甲骨文（Oracle）公司的 MySQL 的适合于分布式计算环境的高实用、高冗余版本。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 Oracle Net 拥有资源、创建表、创建视图、创建过程、Dbfs 角色和网络访问权限，从而破坏数据库文件系统，拥有本地登录特权，登录到调度程序执行的基础设施，从而危及调度程序，导致 Scheduler 被接管，插入或删除对某些 MySQL Cluster 可访问数据的访问，以及未经授权的功能，从而导致 MySQL Cluster 的部分拒绝服务（部分 DOS）等。

CNVD 收录的相关漏洞包括：Oracle Application Express Data Reporter component 权限获取漏洞、Oracle Database Server Database Filesystem component 未授权访问漏洞、Oracle Database Server Express Quick Poll component 权限获取漏洞、Oracle Database

Server Oracle Application Express component 未授权访问漏洞、Oracle Database Server Oracle Text component 未授权访问漏洞、Oracle Database Server Scheduler component 未授权访问漏洞、Oracle Database Server 信息泄露漏洞、Oracle MySQL Cluster Cluster NDBCluster Plugin 拒绝服务漏洞。其中，“Oracle Database Server Scheduler component 未授权访问漏洞”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-2021-00839
https://www.cnvd.org.cn/flaw/show/CNVD-2021-00837
https://www.cnvd.org.cn/flaw/show/CNVD-2021-00835
https://www.cnvd.org.cn/flaw/show/CNVD-2021-00838
https://www.cnvd.org.cn/flaw/show/CNVD-2021-00841
https://www.cnvd.org.cn/flaw/show/CNVD-2021-00842
https://www.cnvd.org.cn/flaw/show/CNVD-2021-00396
https://www.cnvd.org.cn/flaw/show/CNVD-2021-00834

5、SolarWinds Web Help Desk 跨站脚本漏洞（CNVD-2021-01529）

SolarWinds Web Help Desk 是一款基于 Web 的帮助台工单和 IT 资产管理软件。SolarWinds Web Help Desk 12.7.0 存在跨站脚本漏洞。攻击者可通过带有特制 Location Name 字段的 CSV 模板文件利用该漏洞进行跨站脚本攻击。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-2021-01529

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-2021-01563	Agentejo Cockpit NoSQL 注入漏洞	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://github.com/agentejo/cockpit/commit/79fc9631ffa29146e3124ceaf99879b92e1ef24b
CNVD-2021-01561	Agentejo Cockpit NoSQL 注入漏洞（CNVD-2021-01561）	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/agentejo/cockpit/commit/79fc9631ffa29146e3124ceaf99879b92e1ef24b
CNVD-2021-01562	Agentejo Cockpit NoSQL 注入漏洞（CNVD-2021-01562）	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/agentejo/cockpit/com

			mit/79fc9631ffa29146e3124ceaf99879b92e1ef24b
CNVD-2021-01560	Egavilan Media EGM Address Book 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://egavilanmedia.com/egm-address-book/
CNVD-2021-01573	Esri Arcgis Server 服务端请求伪造漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://support.esri.com/en/technical-article/000022931
CNVD-2021-01287	GNU LibreDWG bits.c 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://github.com/LibreDWG/libredwg/commit/b84c2cab55948a5ee70860779b2640913e3ee1ed
CNVD-2021-01286	GNU LibreDWG decode_R13_R2000 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/LibreDWG/libredwg/commit/f878ba67b638f0d5050b6dba61b9737f64fc53de
CNVD-2021-01049	ismartgate PRO 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://ismartgate.com/secure-garage-door/
CNVD-2021-01574	Jiransecurity Spamsniper 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://www.jiransecurity.com/
CNVD-2021-01528	Korzio Djv 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://snyk.io/vuln/SNYK-JS-DJV-1014545

小结：本周，Google 产品被披露存在多个漏洞，攻击者可利用导致所需的系统执行特权在本地升级，导致特权的本地升级，而无需其他执行特权等。此外，Microsoft、IBM、Oracle 等多款产品被披露存在多个漏洞，攻击者可利用在目标系统上执行任意代码，控制受影响的系统，通过 Oracle Net 拥有资源、创建表、创建视图、创建过程、Dbfs 角色和网络访问权限，从而破坏数据库文件系统等。另外，SolarWinds Web Help Desk 被披露存在跨站脚本漏洞。攻击者可通过带有特制 Location Name 字段的 CSV 模板文件利用该漏洞进行跨站脚本攻击。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、Online Marriage Registration System SQL 注入漏洞

验证描述

Online Marriage Registration System 是一个支持在线婚姻登记的建站系统。

Online Marriage Registration System 1.0 版本存在 SQL 注入漏洞，该漏洞源于 search.php 请求 searchdata 参数缺少对外部输入 SQL 语句的验证，攻击者可以利用此漏洞注入获取数据库信息。

验证信息

POC 链接：https://www.exploit-db.com/exploits/49307

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2021-01534

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. Google 修复了 Android 中的关键远程代码执行漏洞

Google 发布了一个 Android 安全更新，解决了 43 个漏洞，其中包括一个跟踪为 CVE-2021-0316 的 Android 系统组件中的关键远程代码执行漏洞。Google 通过发布 2021-01-05 或更高版本的安全补丁程序解决了这些缺陷。

参考链接：https://securityaffairs.co/wordpress/113095/security/google-android-rce.html

2. Nissan 源代码通过配置错误的 Git 服务器泄漏

由于公司 Git 服务器的配置错误，日产北美地区的源代码在线泄漏，该服务器因为默认用户名和密码 admin / admin 而在线暴露。泄漏的信息包括日产移动应用程序的源代码，诊断工具，市场研究工具和数据以及其他资产。

参考链接：https://www.darkreading.com/risk/nissan-source-code-leaked-via-misconfigured-git-server/d/d-id/1339845

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