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 25 日-2021 年 01 月 31 日　　2020 年第 4 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 355 个，其中高危漏洞 117 个、中危漏洞 190 个、低危漏洞 48 个。漏洞平均分值为 5.62。本周收录的漏洞中，涉及 0day 漏洞 173 个（占 49%），其中互联网上出现“SolarWinds Web Help Desk CSV 注入漏洞、Webmin 任意命令执行漏洞（CNVD-2021-07125）”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 5712 个，与上周（6101 个）环比减少 6%。

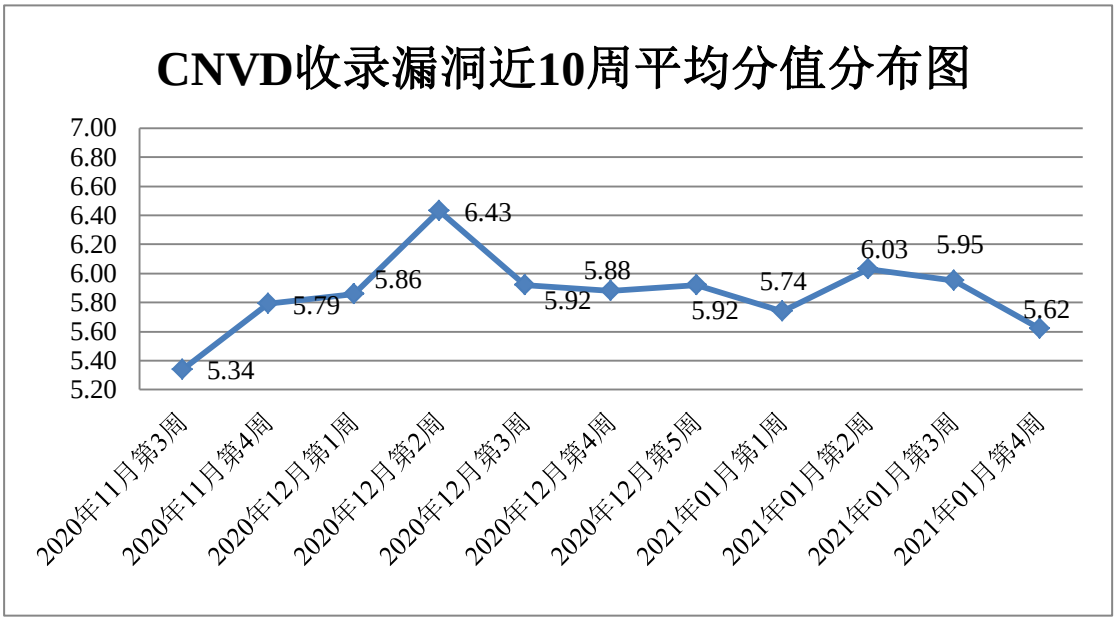

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 12 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 591 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 136 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 17 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：

三菱电机自动化（中国）有限公司、友讯电子设备（上海）有限公司、上海拉扎斯信息科技有限公司、谷歌公司、武汉九二五游网络科技有限公司、深圳市博思协创网络科技有限公司、北京映翰通网络技术股份有限公司、上海鼎莲软件科技有限公司、湖北淘码千维信息科技有限公司、北京辉助共赢科技发展有限公司、常州易奇信息科技有限公司、深圳市必联电子有限公司、广州酷狗计算机科技有限公司、深圳市双梦科技有限公司、北京惠朗时代科技有限公司、北京良精志诚科技有限责任公司、深圳市矽伟智科技有限公司、北京金盘鹏图软件技术有限公司、重庆巨泰物联网集团有限公司、广州市花都区新华伟创广告设计服务部、南京酷奇信息科技有限公司、广州盈可视电子科技有限公司、许昌永诚网络科技有限公司、太原迅易科技有限公司、广州齐博网络科技有限公司、广东凯格科技有限公司、微软(中国)有限公司、陕西锦华网络科技有限责任公司、广州市奥威亚电子科技有限公司、成都星锐蓝海网络科技有限公司、山西牛酷信息科技有限公司、用友网络科技股份有限公司、北京翼鸥教育科技有限公司、济南宇霞信息技术有限公司、北京心往科技有限公司、山东畅想云教育科技有限公司、北京怡和信技术服务有限公司、普联技术有限公司、深圳创维数字技术有限公司、沈阳点动科技有限公司、深圳市昂捷信息技术有限公司、成都时代汇创科技有限公司、北京致远互联软件有限公司、北京国炬信息技术有限公司、深圳警翼智能科技股份有限公司、合肥市道克莱尔信息科技有限公司、廊坊市极致网络科技有限公司、苏州汇川技术有限公司、华硕电脑（上海）有限公司、湖南快乐阳光互动娱乐传媒有限公司、北京智邦国际软件技术有限公司、深圳市迅捷通信技术有限公司、用友网络科技有限公司、广州网易计算机系统有限公司、安徽小皮教育科技有限公司、南京九则软件科技有限公司、畅捷通信息技术股份有限公司、北京南北天地科技股份有限公司、北京大米科技有限公司、北京致远互联软件股份有限公司、上海孚盟软件有限公司、山东城通科技有限公司、西安昊博智能科技公司、武汉小咪网络科技有限公司、成都奇鲁科技有限公司、湖南一唯信息科技有限公司、上海纵之格科技有限公司、北京天星组态软件有限公司、浙江易舸软件有限公司、北京星网锐捷网络技术有限公司、武汉京伦科技有限公司、杭州恩软信息技术有限公司、安徽渔之蓝教育软件技术有限公司、东莞市同享软件科技有限公司、上海喜马拉雅科技有限公司、南瑞集团有限公司、广州红帆电脑科技有限公司、锐捷网络股份有限公司、博文教育（亞洲）有限公司、浪潮集团有限公司、《中国学术期刊（光盘版）》电子杂志社有限公司、昆明云涛科技有限公司、深圳市美科星通信技术有限公司、北京邦永科技有限公司、石家庄捷搜网络科技有限公司、海南翼智慧信息科技有限公司、深圳

市易通鼎多媒体有限公司、淄博闪灵网络科技有限公司、深圳市锟锆科技有限公司、南京极域信息科技有限公司、天融信科技集团、小米科技有限责任公司、武汉京伦科技开发有限公司、金蝶软件、智睿软件、米酷资源网、飞飞影视导航系统、雷风影视、北京为因软件、梦想 cms、熊海 CMS 、Excitel Broadband Pvt. Ltd.、MessageSolution, Inc.、FibRSol、suraajcomputer、Apache Friends、ZZCMS、Z-Blog、Guojiz、MessageSolution、Bandisoft、HadSky、MayiCMS、SIEMENS 和 WordPress。

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、北京数字观星科技有限公司、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。远江盛邦（北京）网络安全科技股份有限公司、南京众智维信息科技有限公司、国瑞数码零点实验室、北京华云安信息技术有限公司、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、山东新潮信息技术有限公司、山东云天安全技术有限公司、北京天地和兴科技有限公司、山东华鲁科技发展股份有限公司、河南灵创电子科技有限公司 、河南信安世纪科技有限公司、内蒙古奥创科技有限公司、新疆海狼科技有限公司、杭州海康威视数字技术股份有限公司、安徽长泰信息安全服务有限公司、北京信联科汇科技有限公司、福建省海峡信息技术有限公司、江苏保旺达软件技术有限公司、京东云安全、贵州多彩宝互联网服务有限公司、北京时代新威信息技术有限公司、北京圣博润高新技术股份有限公司、北京机沃科技有限公司、北京惠而特科技有限公司、广州市蓝爵计算机科技有限公司、北京中科微澜科技有限公司、上海观安信息技术股份有限公司、山东道普测评技术有限公司、北京长亭科技有限公司、上海纽盾科技股份有限公司、河南省鼎信信息安全等级测评有限公司、北京智游网安科技有限公司、广州安亿信软件科技有限公司、广州市云聚数据服务有限公司、武汉明嘉信信息安全检测评估有限公司、四川哨兵信息科技有限公司、南京节点安全技术有限公司及其他个人白帽子向 CNVD 提交了 5712 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 3511 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）	2264	2264
上海交大	735	735
奇安信网神（补天平台）	512	512
北京天融信网络安全技术有限公司	285	2
哈尔滨安天科技集团股份有	237	0

限公司		
北京神州绿盟科技有限公司	136	5
北京数字观星科技有限公司	109	0
深信服科技股份有限公司	86	0
北京启明星辰信息安全技术有限公司	77	22
新华三技术有限公司	73	0
华为技术有限公司	47	0
中国电信集团系统集成有限责任公司	42	42
杭州安恒信息技术股份有限公司	30	30
中国电信股份有限公司网络安全产品运营中心	20	0
北京知道创宇信息技术股份有限公司	6	0
恒安嘉新(北京)科技股份公司	5	0
远江盛邦（北京）网络安全科技股份有限公司	584	584
南京众智维信息科技有限公司	228	228
北京华顺信安科技有限公司	184	0
国瑞数码零点实验室	96	96
北京华云安信息技术有限公司	73	73
北京山石网科信息技术有限公司	72	72
上海犀点意象网络科技有限公司	48	48
山东新潮信息技术有限公司	43	43
山东云天安全技术有限公司	36	36
北京天地和兴科技有限公司	35	35
山东华鲁科技发展股份有限公司	32	32
河南灵创电子科技有限公司	30	30
河南信安世纪科技有限公司	24	24
内蒙古奥创科技有限公司	20	20
杭州迪普科技股份有限公司	18	0
新疆海狼科技有限公司	17	17
杭州海康威视数字技术股份有限公司	17	17
安徽长泰信息安全服务有限	16	16

公司		
北京信联科汇科技有限公司	13	13
福建省海峡信息技术有限公司	10	10
江苏保旺达软件技术有限公司	10	10
京东云安全	9	9
贵州多彩宝互联网服务有限公司	7	7
北京时代新威信息技术有限公司	7	7
北京圣博润高新技术股份有限公司	6	6
北京机沃科技有限公司	6	6
北京惠而特科技有限公司	6	6
广州市蓝爵计算机科技有限公司	5	5
北京中科微澜科技有限公司	4	4
上海观安信息技术股份有限公司	3	3
山东道普测评技术有限公司	2	2
北京长亭科技有限公司	2	2
上海纽盾科技股份有限公司	2	2
河南省鼎信信息安全等级测评有限公司	1	1
北京智游网安科技有限公司	1	1
广州安亿信软件科技有限公司	1	1
广州市云聚数据服务有限公司	1	1
武汉明嘉信信息安全检测评估有限公司	1	1
四川哨兵信息科技有限公司	1	1
南京节点安全技术有限公司	1	1
CNCERT 青海分中心	11	11
CNCERT 上海分中心	10	10
CNCERT 河北分中心	8	8
CNCERT 重庆分中心	7	7
CNCERT 西藏分中心	7	7
CNCERT 浙江分中心	6	6
CNCERT 天津分中心	3	3
CNCERT 宁夏分中心	3	3
CNCERT 山东分中心	1	1

个人	574	574
报送总计	6966	5712

本周漏洞按类型和厂商统计

本周，CNVD 收录了 355 个漏洞。应用程序 221 个，WEB 应用 84 个，网络设备（交换机、路由器等网络端设备）33 个，智能设备（物联网终端设备）6 个，操作系统 6 个，安全产品 5 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	221
WEB 应用	84
网络设备（交换机、路由器等网络端设备）	33
智能设备（物联网终端设备）	6
操作系统	6
安全产品	5

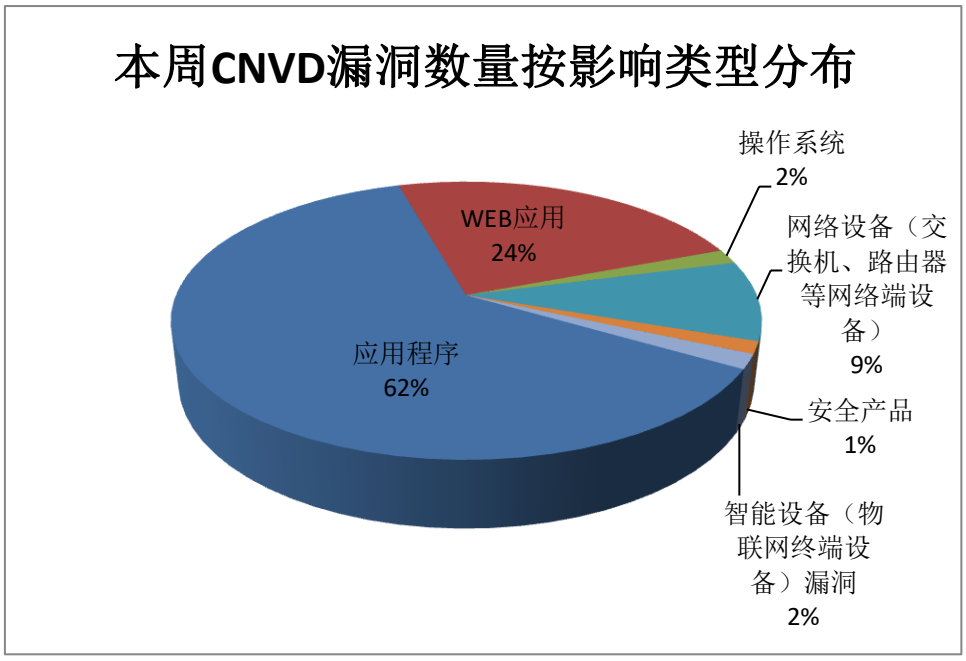

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Cisco、Google、西门子（中国）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	Cisco	21	6%
2	Google	20	6%

3	西门子（中国）有限公司	17	5%
4	IBM	16	5%
5	Oracle	14	4%
6	北京搜狗信息服务有限公司	12	3%
7	Quest	11	3%
8	佳佳软件	9	2%
9	Mozilla	9	2%
10	其他	226	64%

本周行业漏洞收录情况

本周，CNVD 收录了 25 个电信行业漏洞，13 个移动互联网行业漏洞，34 个工控行业漏洞（如下图所示）。其中，“锐捷网关存在未授权访问漏洞”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/

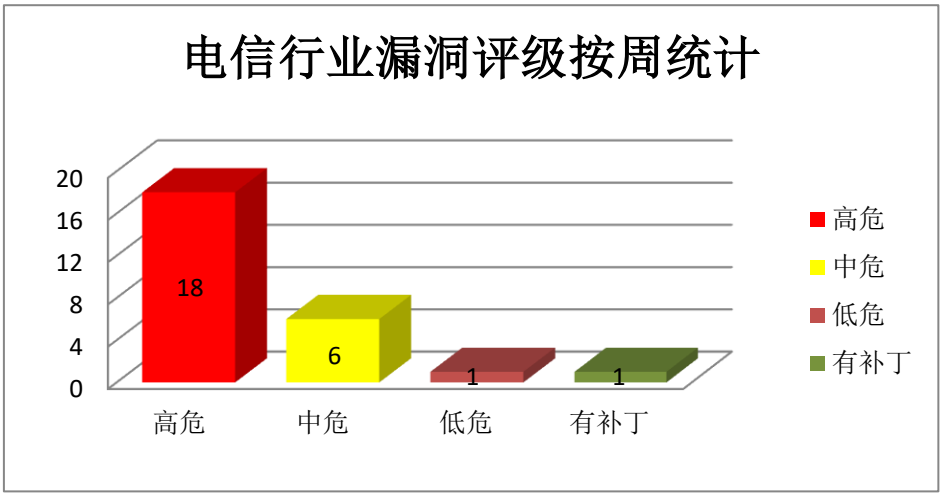

图 3 电信行业漏洞统计

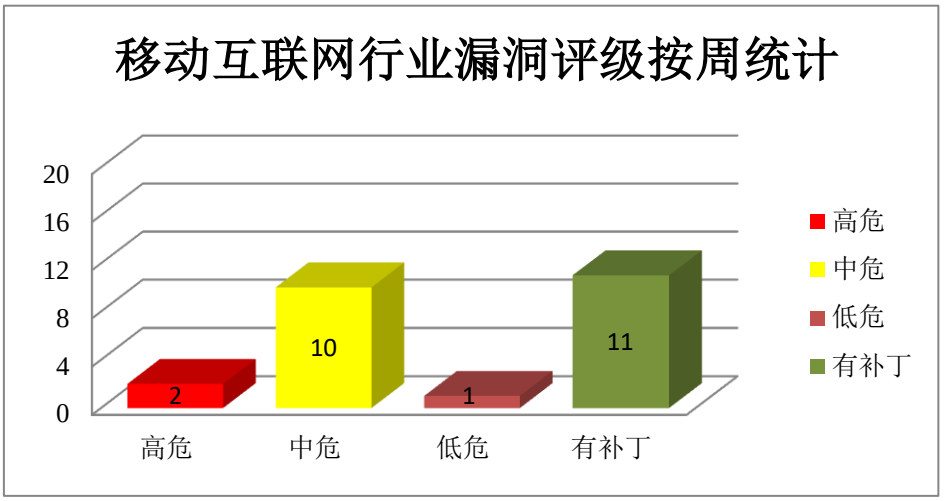

图 4 移动互联网行业漏洞统计

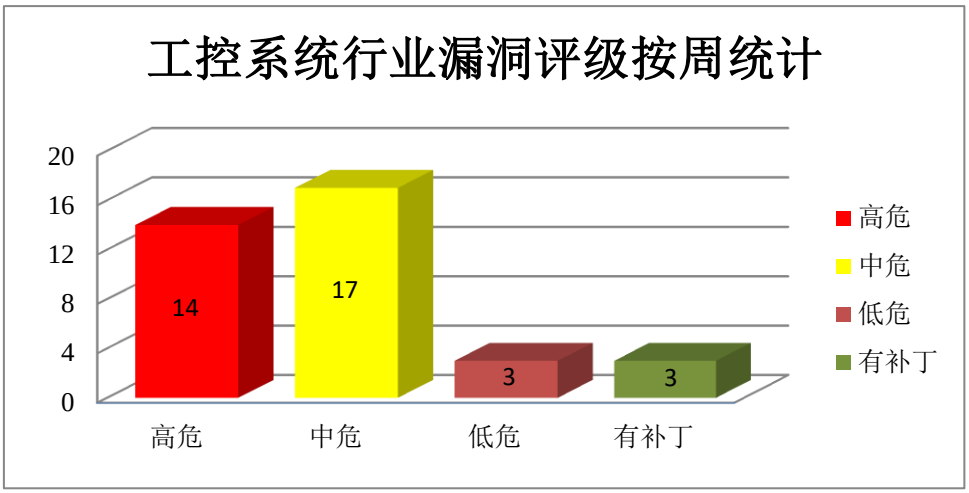

图 5 工控系统行业漏洞统计

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。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 页面绕过防火墙控制，利用堆破坏，执行沙箱转义等。

CNVD 收录的相关漏洞包括：Google Chrome 堆缓冲区溢出漏洞（CNVD-2021-07099）、Google Chrome ImageBurner 竞争条件漏洞、Google Chrome 联网策略执行不足漏洞（CNVD-2021-07102）、Google Chrome WASM 数据验证不足漏洞、Google Chrome 释放后重用漏洞（CNVD-2021-07100、CNVD-2021-07105）、Google Chrome V8 实现不当漏洞（CNVD-2021-07106）、Google Chrome cryptohome 实现不当漏洞。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-2021-07099

https://www.cnvd.org.cn/flaw/show/CNVD-2021-07103

https://www.cnvd.org.cn/flaw/show/CNVD-2021-07102

https://www.cnvd.org.cn/flaw/show/CNVD-2021-07101

https://www.cnvd.org.cn/flaw/show/CNVD-2021-07100

https://www.cnvd.org.cn/flaw/show/CNVD-2021-07106

https://www.cnvd.org.cn/flaw/show/CNVD-2021-07105

https://www.cnvd.org.cn/flaw/show/CNVD-2021-07104

2、Cisco 产品安全漏洞

Cisco AnyConnect Secure Mobility Client for Windows 是一款基于 Windows 平台的可通过任何设备安全访问网络和应用的安全移动客户端。Cisco Security Manager（CSM）是一套企业级的管理应用，它主要用于在 Cisco 网络和安全设备上配置防火墙、VPN 和入侵保护安全服务。Cisco Expressway 是一款网关解决方案，可让您的防火墙之外的用户简单、高度安全地访问所有协同工作。Cisco Firepower Management Center（FMC）是新一代防火墙管理中心软件。Cisco Edge Fog Fabric（EFF）是面向工业客户的开放架构物联网平台。Cisco TelePresence Collaboration Endpoint（CE）是一款使用在 Cisco 视频会议解决方案中的协作终端软件。Cisco AnyConnect Secure Mobility Client 是一种虚拟专用网络（VPN）客户端，适用于各种操作系统和硬件配置。Nexus Data Broker 提供了一种针对大流量和关键业务流量的简单、可扩展且具有成本效益的监视解决方案。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞未经授权获得网络访问权限，覆盖任意文件，导致拒绝服务等。

CNVD 收录的相关漏洞包括：Cisco AnyConnect Secure Mobility Client for Windows 代码问题漏洞（CNVD-2021-05520）、Cisco Security Manager 路径遍历漏洞、Cisco Expressway Software 信息泄露漏洞、Cisco Firepower Management Center 拒绝服务漏洞、Cisco Edge Fog Fabric 授权问题漏洞 、Cisco TelePresence Collaboration Endpoint 访问控制错误漏洞、Cisco AnyConnect Secure Mobility Client for Windows 拒绝服务漏洞、Cisco Nexus Data Broker Software 路径遍历漏洞。其中，“Cisco AnyConnect Secure Mobility Client for Windows 代码问题漏洞（CNVD-2021-05520）”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-2021-05520

https://www.cnvd.org.cn/flaw/show/CNVD-2021-05530

https://www.cnvd.org.cn/flaw/show/CNVD-2021-05529

https://www.cnvd.org.cn/flaw/show/CNVD-2021-05533

https://www.cnvd.org.cn/flaw/show/CNVD-2021-05532

https://www.cnvd.org.cn/flaw/show/CNVD-2021-05531

https://www.cnvd.org.cn/flaw/show/CNVD-2021-05539

https://www.cnvd.org.cn/flaw/show/CNVD-2021-05535

3、IBM 产品安全漏洞

IBM WebSphere Application Server（WAS）是由 IBM 遵照开放标准，例如 Java EE、XML 及 Web Services，开发并发行的一种应用服务器。IBM Security Identity Governance and Intelligence（IGI）是一套身份管理和治理解决方案。IBM Planning Analytics 是美国 IBM 公司的一套业务规划分析解决方案。IBM Spectrum LSF Suite 是美国 IBM 公司的一套工作负载管理解决方案。IBM Security Guardium Data Encryption (GDE)提供了一组模块化的加密解决方案，可帮助安全团队有效地实现整个组织的静态数据安全性。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞绕过身份验证，获取敏感信息或消耗内存资源等。

CNVD 收录的相关漏洞包括：IBM WebSphere Application Server XML 外部实体注入漏洞（CNVD-2021-06634）、IBM Security Identity Governance 身份验证漏洞、IBM Security Identity Governance and Intelligence 信息泄露漏洞、IBM Planning Analytics 信息泄露漏洞（CNVD-2021-06640、CNVD-2021-06639）、IBM Spectrum LSF 命令注入漏洞、IBM Security Guardium Data Encryption 权限控制不当漏洞、IBM Security Guardium Data Encryption 弱加密算法漏洞。其中，“IBM WebSphere Application Server XML 外部实体注入漏洞（CNVD-2021-06634）、IBM Security Identity Governance 身份验证漏洞”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-2021-06634

https://www.cnvd.org.cn/flaw/show/CNVD-2021-06635

https://www.cnvd.org.cn/flaw/show/CNVD-2021-06641

https://www.cnvd.org.cn/flaw/show/CNVD-2021-06640

https://www.cnvd.org.cn/flaw/show/CNVD-2021-06639

https://www.cnvd.org.cn/flaw/show/CNVD-2021-06638

https://www.cnvd.org.cn/flaw/show/CNVD-2021-06645

https://www.cnvd.org.cn/flaw/show/CNVD-2021-06644

4、Huawei 产品安全漏洞

Huawei Mate 30 是一款智能手机。Huawei Taurus-AL00A 是一款智能手机。"Huawei Taurus-AL00A 是一款智能手机。Huawei Taurus-AL00A 是一款智能手机。Huawei Manageone 是一套云数据中心管理解决方案。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞导致缓冲区溢出，影响设备正常使用等。

CNVD 收录的相关漏洞包括：Huawei Mate 30 缓冲区溢出漏洞（CNVD-2021-07518）、Huawei Mate 30 弱算法漏洞（CVE-2021-22307）、Huawei Taurus-AL00A 内存错误引用漏洞、Huawei Taurus-AL00A 越界读取漏洞、Huawei Taurus-AL00A 指针双重释放漏洞、Huawei ManageOne CSV 注入漏洞、Huawei Mate 30 越界读取漏洞（CNVD-2021-07520）、Huawei Mate 30 栈溢出漏洞。其中，“Huawei Mate 30 缓冲区溢出漏洞（CNVD-2021-07518）、Huawei ManageOne CSV 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-2021-07518
https://www.cnvd.org.cn/flaw/show/CNVD-2021-07517
https://www.cnvd.org.cn/flaw/show/CNVD-2021-07516
https://www.cnvd.org.cn/flaw/show/CNVD-2021-07515
https://www.cnvd.org.cn/flaw/show/CNVD-2021-07514
https://www.cnvd.org.cn/flaw/show/CNVD-2021-07521
https://www.cnvd.org.cn/flaw/show/CNVD-2021-07520
https://www.cnvd.org.cn/flaw/show/CNVD-2021-07519

5、Quest Policy Authority 跨站脚本漏洞

Quest Policy Authority For Unified Communications 是美国 Quest 公司的一个用于企业环境中整合各种媒体之间的通信数据（文本和即时消息，视频会议，电子邮件和语音邮件）的软件。本周，Quest Policy Authority 被披露存在跨站脚本漏洞。攻击者可利用该漏洞通过 PolicyAuthority/Common/FolderControl.jsp 的 unqID 参数向浏览器注入恶意代码。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-2021-07073

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-2021-06535	The Guild Graphql Tools 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://github.com/ardatan/graphql-tools/commit/6a966beee8ca8b2f4adfe93318b96e4a5c501eac
CNVD-2021-06534	PrestaShop SQL 注入漏洞（CNVD-2021-06534）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.prestashop.com/en

CNVD-2021-06543	Lukeed dset 原型污染漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/lukeed/dset/blob/50a6ead172d1466a96035eff00f8eb465ccd050a/src/index.js#L6
CNVD-2021-06866	NVIDIA SHIELD TV 权限提升漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://nvidia.custhelp.com/app/answers/detail/a_id/5148
CNVD-2021-06950	HGiga MailSherlock 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.twcert.org.tw/en/cp-139-4264-f10f4-2.html
CNVD-2021-07059	锐捷网关存在未授权访问漏洞	高	厂商已发布相关漏洞补丁链接，请关注厂商主页及时更新：http://www.ruijie.com.cn/
CNVD-2021-07092	picoTCP 越界写入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://us-cert.cisa.gov/ics/advisories/icsa-20-343-01
CNVD-2021-07113	NVIDIA SHIELD TV NVDEC 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://nvidia.custhelp.com/app/answers/detail/a_id/5148
CNVD-2021-07121	Zyxel USG Series 凭据泄露漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://businessforum.zyxel.com/discussion/5254/whats-new-for-zld4-60-patch-1-available-on-dec-15
CNVD-2021-07120	Zyxel SD-OS chg_exp_pwd 输入验证漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.zyxel.com/support/Zyxel-security-advisory-for-command-injection-vulnerability-of-firewalls.shtml

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 页面绕过防火墙控制，利用堆破坏，执行沙箱转义等。此外，Cisco、IBM、Huawei 等多款产品被披露存在多个漏洞，攻击者可利用漏洞未经授权获得网络访问权限，覆盖任意文件，获取敏感信息或消耗内存资源等。另外，Quest Policy Authority 被披露存在跨站脚本漏洞。攻击者可利用该漏洞通过 PolicyAuthority/Common/FolderControl.jsp 的 unqID 参数向浏览器注入恶意代码。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、SolarWinds Web Help Desk CSV 注入漏洞

验证描述

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 CSV 注入漏洞。攻击者可通过附加到工单的文件利用该漏洞进行 CSV 注入攻击。

验证信息

POC 链接：https://github.com/pixelimity/pixelimity/issues/20

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2021-06945

信息提供者

北京天融信网络安全技术有限公司

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. 新的 Docker 容器转义漏洞影响 Microsoft Azure 功能

Microsoft Azure Functions 中未修补的漏洞被披露，攻击者可以利用该漏洞提权并逃脱用于托管特权的 Docker 容器。

参考链接：https://thehackernews.com/2021/01/new-docker-container-escape-bug-affects.html

2. TikTok 漏洞可能暴露用户的个人资料数据和电话号码

网络安全研究人员披露了 TikTok 中现已修复的安全漏洞，该漏洞可能使攻击者能够建立该应用程序的用户及其关联电话号码的数据库，用于将来的恶意活动。

参考链接：https://thehackernews.com/2021/01/tiktok-bug-could-have-exposed-users.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