国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2020 年 12 月 21 日-2020 年 12 月 27 日　　2020 年第 52 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 298 个，其中高危漏洞 117 个、中危漏洞 128 个、低危漏洞 53 个。漏洞平均分值为 5.88。本周收录的漏洞中，涉及 0day 漏洞 165 个（占 55%），其中互联网上出现“Mitel ShoreTel conferencing component 跨站脚本漏洞、CloudBees Jenkins Dependency Graph Viewer 插件跨站脚本漏洞”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 11489 个，与上周（12185 个）环比减少 6%。

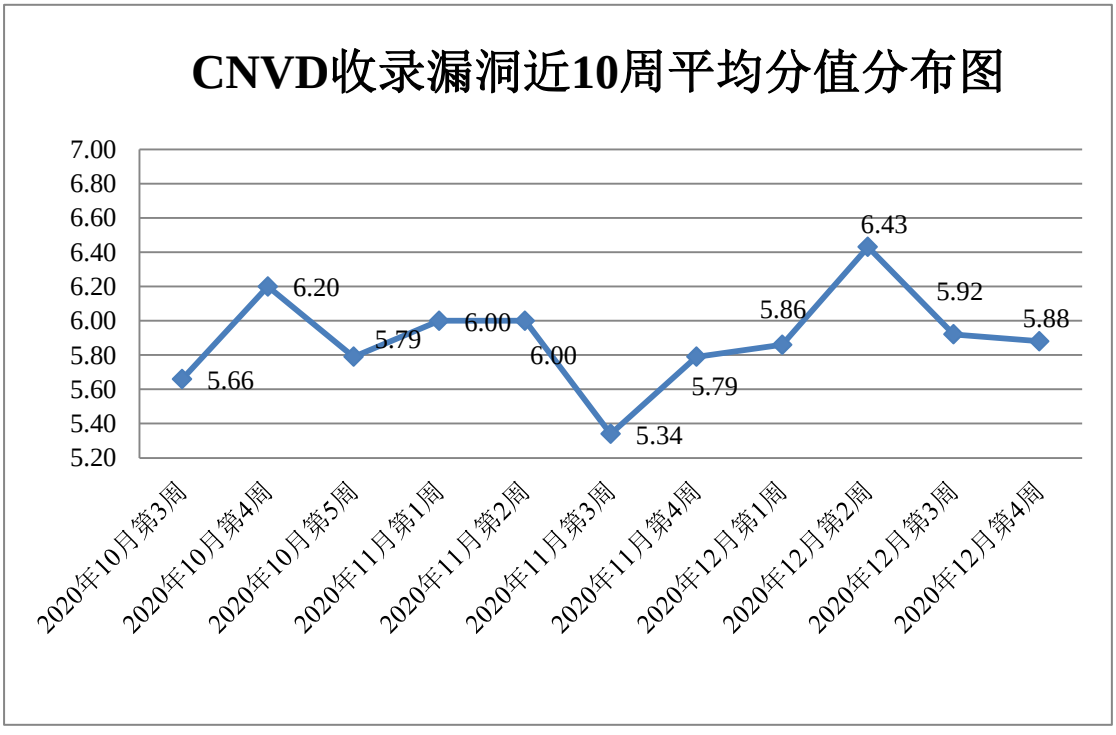

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 25 起，向基础电信企业通报漏洞事件 5 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 415 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 75 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 33 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：

杭州伊柯夫科技有限公司、北京爱迪科森教育科技股份有限公司、上海亿速网络科技有限公司、四川清和科技有限公司、罗克韦尔自动化（中国）有限公司、南京酷奇信息科技有限公司、上海格诗网络科技有限公司、北京猎豹网络科技有限公司、四川万博教育软件股份有限公司、上海讯有信息科技有限公司、常州文庭软件有限公司、深圳点猫科技有限公司、益盟股份有限公司、广东大比特资讯广告发展有限公司、北京多点在线科技有限公司、北京神奇像素科技有限公司、天津时光印记文化传播有限公司、深圳昱途网络科技有限公司、北京坤豆科技有限公司、华安证券股份有限公司、武汉华中数控股份有限公司、广州红帆科技有限公司、深圳维盟科技股份有限公司、北京江伟时代科技有限公司、北京欧倍尔软件技术开发有限公司、杭州默安科技有限公司、北京致远互联软件股份有限公司、金蝶软件（中国）有限公司、上海纵之格科技有限公司、淄博闪灵网络科技有限公司、宿州市涛盛网络科技有限公司、世纪星网络信息服务有限公司、深圳市蓝凌软件股份有限公司、中科软股教育科技（北京）股份有限公司、湖南翱云网络科技有限公司、苏州汇川技术有限公司、广州易城网络科技股份有限公司、帆软软件有限公司、广州市国万电子科技有限公司、广州联雅网络科技有限公司、北京网易有道计算机系统有限公司、南京科远自动化集团股份有限公司、山西龙采科技有限公司阳泉分公司、北京瑞星网安技术股份有限公司、深圳市常青藤软件科技有限公司、金蝶国际软件集团有限公司、上海商派网络科技有限公司、小船出海教育科技（北京）有限公司、广州中望龙腾软件股份有限公司、中电鸿信信息科技有限公司、深圳市爱思软件技术有限公司、成都飞鱼星科技股份有限公司、浙江大华技术股份有限公司、安徽小皮教育科技有限公司、南京千目信息科技有限公司、广州图创计算机软件开发有限公司、南京大众书网图书文化有限公司、北京百合小两口信息技术有限公司上海分公司、河北白晶环境科技有限公司、厦门科拓通讯技术股份有限公司、广州网易计算机系统有限公司、深圳市爱德数智科技股份有限公司、四川思途智旅软件有限公司、北京世纪飞育软件有限责任公司、北京猿力教育科技有限公司、安徽康海时代科技股份有限公司、武汉木仓科技股份有限公司、施耐德电气、米酷资源网、北京引领盛世网络科技发展中心、若依、Python 软件基金会、、DedeBIZ、MayiCMS、UQCMS、Catfishcms、UCMS、Check Point Software Technologies、zzzcms、Hancom。

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、厦门服云信息科技有限公司、北京神州绿盟科技有限公司、中国电信集团系统集成有限责任公司等单位报送公开收集的漏洞数量较多。国瑞数码零点实验室、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、新疆海狼科技有限公司、河南灵创电子科技有限公司 、山东华鲁科技发展股份有限公司、内蒙古奥创科技有限公司、河南信安世纪科技有限公司、杭州迪普科技股份有限公司、山东云天安全技术有限公司、长扬科技（北京）有限公司、北京赛克艾威科技有限公司、山东新潮信息技术有限公司、北京网御星云信息技术有限公司、北京云科安信科技有限公司（Seraph 安全实验室）、北京机沃科技有限公司、远江盛邦（北京）网络安全科技股份有限公司、上海观安信息技术股份有限公司、广州市蓝爵计算机科技有限公司、北京惠而特科技有限公司、北京零零信安科技有限公司、京东云安全、山东道普测评技术有限公司、工业信息安全(四川)创新中心有限公司、湖南省金盾信息安全等级保护评估中心有限公司、江苏茴香豆网络科技有限公司、星云博创科技有限公司、钉钉科技有限公司、浙江安腾信息技术有限公司、北京智游网安科技有限公司、杭州漠坦尼科技有限公司、上海市信息安全测评认证中心、湖南长城信息金融设备有限责任公司及其他个人白帽子向 CNVD 提交了 11489 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 9989 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）	7675	7675
斗象科技（漏洞盒子）	1837	1837
上海交大	477	477
北京天融信网络安全技术有限公司	308	6
哈尔滨安天科技集团股份有限公司	274	0
厦门服云信息科技有限公司	251	0
北京神州绿盟科技有限公司	233	0
中国电信集团系统集成有限责任公司	120	120
新华三技术有限公司	87	0
深信服科技股份有限公司	80	0
华为技术有限公司	80	0
北京启明星辰信息安全技术有限公司	71	21
北京数字观星科技有限公司	50	0

中国电信股份有限公司网络安全产品运营中心	20	0
西安四叶草信息技术有限公司	17	17
北京知道创宇信息技术股份有限公司	2	0
国瑞数码零点实验室	129	129
北京山石网科信息技术有限公司	66	66
南京众智维信息科技有限公司	61	61
北京天地和兴科技有限公司	58	58
新疆海狼科技有限公司	58	58
河南灵创电子科技有限公司	54	54
山东华鲁科技发展股份有限公司	47	47
内蒙古奥创科技有限公司	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	14	0
山东云天安全技术有限公司	14	14
长扬科技（北京）有限公司	12	12
北京赛克艾威科技有限公司	11	11
山东新潮信息技术有限公司	11	11
北京网御星云信息技术有限公司	10	10
北京云科安信科技有限公司（Seraph 安全实验室）	10	10
北京机沃科技有限公司	9	9
远江盛邦（北京）网络安全科技股份有限公司	9	9
上海观安信息技术股份有限公司	5	5
广州市蓝爵计算机科技有限公司	4	4
北京惠而特科技有限公司	4	4
北京零零信安科技有限公司	4	4
京东云安全	4	4
山东道普测评技术有限公司	4	4
工业信息安全(四川)创新中心有限公司	2	2
湖南省金盾信息安全等级保护评估中心有限公司	2	2
江苏茴香豆网络科技有限公	2	2

司		
星云博创科技有限公司	2	2
钉钉科技有限公司	2	2
浙江安腾信息技术有限公司	2	2
北京智游网安科技有限公司	1	1
杭州漠坦尼科技有限公司	1	1
上海市信息安全测评认证中心	1	1
湖南长城信息金融设备有限责任公司	1	1
CNCERT 宁夏分中心	11	11
CNCERT 贵州分中心	3	3
CNCERT 四川分中心	3	3
CNCERT 海南分中心	1	1
个人	685	685
报送总计	12932	11489

本周漏洞按类型和厂商统计

本周，CNVD 收录了 298 个漏洞。应用程序 121 个，WEB 应用 96 个，操作系统 32 个，安全产品 29 个，网络设备（交换机、路由器等网络端设备）15 个，智能设备（物联网终端设备）3 个，数据库 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	121
WEB 应用	96
操作系统	32
安全产品	29
网络设备（交换机、路由器等网络端设备）	15
智能设备（物联网终端设备）	3
数据库	2

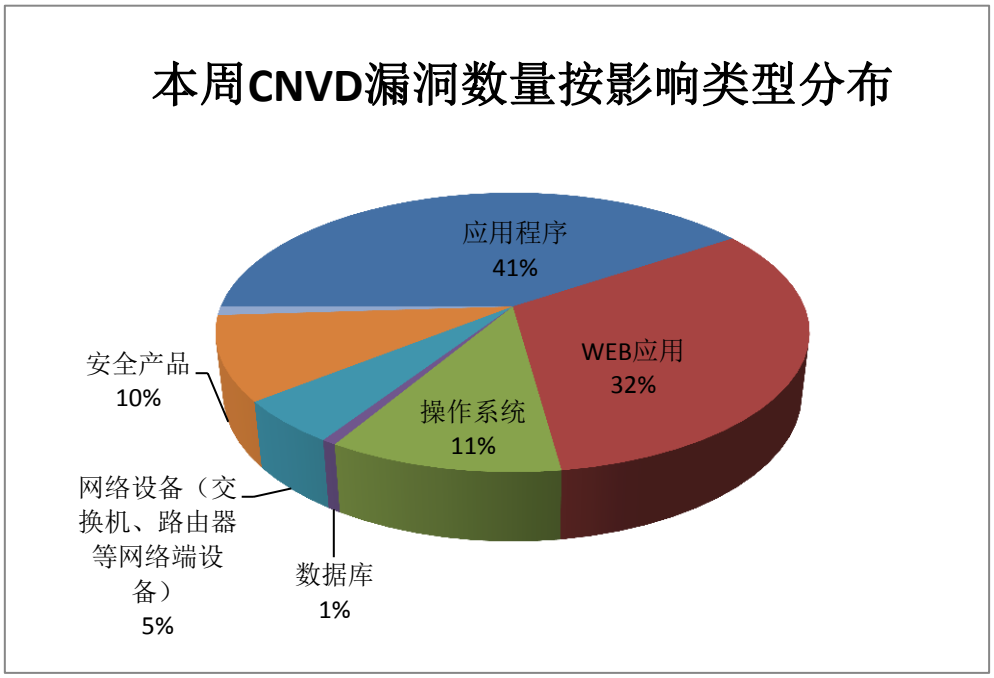

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Google、Trend Micro、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	Google	27	9%
2	Trend Micro	20	7%
3	IBM	16	5%
4	Microsoft	11	4%
5	Solarwinds	9	3%
6	NZXT	7	2%
7	tangro	6	2%
8	MediaWiki	5	2%
9	Odoo	5	2%
10	其他	192	64%

本周行业漏洞收录情况

本周，CNVD 收录了 12 个电信行业漏洞，39 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，“D-Link DSL-2888A 操作系统命令执行漏洞、SolarWinds Orion Network Performance Monitor 权限许可和访问控制问题漏洞、IBM Loopback 注入漏洞”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/

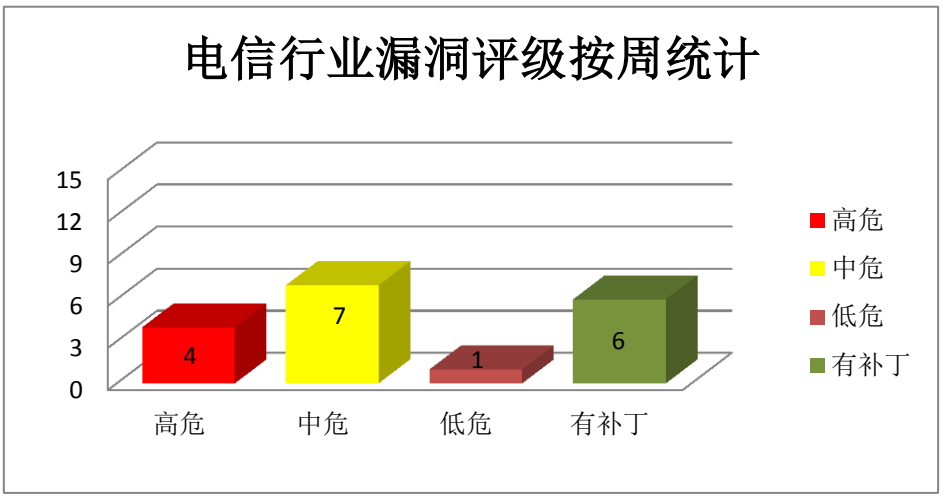

图 3 电信行业漏洞统计

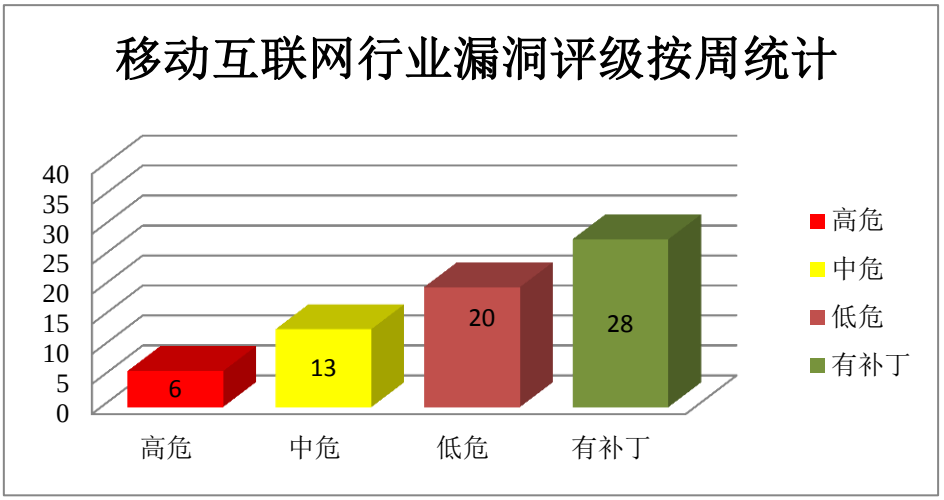

图 4 移动互联网行业漏洞统计

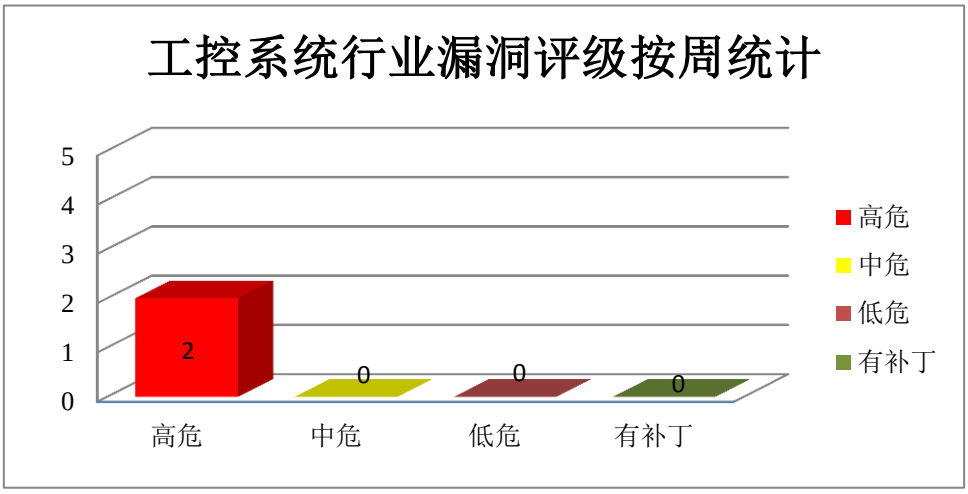

图 5 工控系统行业漏洞统计

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、IBM 产品安全漏洞

IBM Connect：Direct for UNIX 是美国 IBM 公司的一个点对点的可支持多平台之间传输数据的工具软件。IBM Domino 是美国 IBM 公司的一套企业级应用程序开发平台。IBM AIX 是美国 IBM 公司的一款为 IBM Power 体系架构开发的一种基于开放标准的 UNIX 操作系统。IBM VIOS 是一款虚拟 IO 服务器。IBM Loopback 是美国 IBM 公司的一个基于 NodeJs 的 API 框架。IBM Security Key Lifecycle Manager（前称 Tivoli Key Lifecycle Manager）是美国 IBM 公司的一套密钥生命周期管理软件。IBM Financial Transaction Manager for SWIFT Services for Multiplatforms 是美国 IBM 公司的一款金融事务管理器产品。IBM Financial Transaction Manager for SWIFT Services 是美国 IBM 公司的一款金融事务管理器产品。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞访问经过认证的 CLI 会话，破坏服务器或向系统注入代码，ksu 用户命令可获得 root 特权等。

CNVD 收录的相关漏洞包括：IBM Connect:Direct for UNIX 授权问题漏洞、IBM Domino 缓冲区溢出漏洞（CNVD-2020-73021）、IBM AIX 和 VIOS 授权问题漏洞、IBM Loopback 注入漏洞、IBM Security Key Lifecycle Manager 信息泄露漏洞（CNVD-2020-73012）、IBM Financial Transaction Manager for SWIFT Services for Multiplatforms 信息泄露漏洞（CNVD-2020-73014、CNVD-2020-73018）、IBM Financial Transaction Manager for SWIFT Services for Multiplatforms 跨站请求伪造漏洞。其中，“IBM Connect:Direct for UNIX 授权问题漏洞、IBM Domino 缓冲区溢出漏洞（CNVD-2020-73021）、IBM AIX 和 VIOS 授权问题漏洞、IBM Loopback 注入漏洞”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-2020-73022
https://www.cnvd.org.cn/flaw/show/CNVD-2020-73021
https://www.cnvd.org.cn/flaw/show/CNVD-2020-73019
https://www.cnvd.org.cn/flaw/show/CNVD-2020-73497
https://www.cnvd.org.cn/flaw/show/CNVD-2020-73012
https://www.cnvd.org.cn/flaw/show/CNVD-2020-73014
https://www.cnvd.org.cn/flaw/show/CNVD-2020-73013
https://www.cnvd.org.cn/flaw/show/CNVD-2020-73018

2、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，攻击者可利用漏洞获取敏感信息，造成拒绝服务等。

CNVD 收录的相关漏洞包括：Google Android 信息泄露漏洞（CNVD-2020-73454、CNVD-2020-73442、CNVD-2020-73440）、Google Android 输入验证错误漏洞、Google Android 缓冲区溢出漏洞（CNVD-2020-73452、CNVD-2020-73447、CNVD-2020-73446）、Google Android Pixel 拒绝服务漏洞。上述漏洞的综合评级为“中危”。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-2020-73454
https://www.cnvd.org.cn/flaw/show/CNVD-2020-73442
https://www.cnvd.org.cn/flaw/show/CNVD-2020-73440
https://www.cnvd.org.cn/flaw/show/CNVD-2020-73430
https://www.cnvd.org.cn/flaw/show/CNVD-2020-73452
https://www.cnvd.org.cn/flaw/show/CNVD-2020-73447
https://www.cnvd.org.cn/flaw/show/CNVD-2020-73446
https://www.cnvd.org.cn/flaw/show/CNVD-2020-73453

3、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 是一套个人设备使用的操作系统。Microsoft Windows Server 是一套服务器操作系统。Microsoft Excel 是 Microsoft 公司的办公软件 Microsoft office 的组件之一，是一款电子表格程序。Microsoft Azure Sphere 是美国微软（Microsoft）公司的一个应用于云环境提供安全防护的设备。SharePoint 是一款与 Microsoft Office 集成的基于 Web 的协作平台。Microsoft Exchange Server 是 Microsoft 开发的邮件服务器和日历服务器。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞实现远程代码执行，执行使用 PACKET_MMAP 触发漏洞的 shellcode 等。

CNVD 收录的相关漏洞包括：Microsoft Windows/Windows Server Hyper-V 远程代码执行漏洞、Microsoft Excel 远程代码执行漏洞（CNVD-2020-73769）、Microsoft Azure Sphere 代码执行漏洞、Microsoft SharePoint 远程代码执行漏洞（CNVD-2020-73768）、Microsoft SharePoint 权限提升漏洞（CNVD-2020-73766）、Microsoft Exchange Server 远程代码执行漏洞（CNVD-2020-73749、CNVD-2020-73748、CNVD-2020-73747）。其中，“Microsoft Windows/Windows Server Hyper-V 远程代码执行漏洞、Microsoft Excel 远程代码执行漏洞（CNVD-2020-73769）、Microsoft Azure Sphere 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-2020-73767

https://www.cnvd.org.cn/flaw/show/CNVD-2020-73769

https://www.cnvd.org.cn/flaw/show/CNVD-2020-73758

https://www.cnvd.org.cn/flaw/show/CNVD-2020-73768

https://www.cnvd.org.cn/flaw/show/CNVD-2020-73766

https://www.cnvd.org.cn/flaw/show/CNVD-2020-73749

https://www.cnvd.org.cn/flaw/show/CNVD-2020-73748

https://www.cnvd.org.cn/flaw/show/CNVD-2020-73747

4、Trend Micro 产品安全漏洞

Trend Micro Security 2020 是美国趋势科技（Trend Micro）公司的一套计算机安全防护软件。Trend Micro InterScan Web Security Virtual Appliance（IWSVA）是美国趋势科技（Trend Micro）公司的一款针对基于 Web 方式的威胁为企业网络提供动态的、集成式的安全保护的 Web 安全网关。Trend Micro Worry-Free Business Security 是美国趋势科技（Trend Micro）公司的一套企业级信息安全防护解决方案。该产品提供反垃圾邮件、防病毒、网络安全和电子邮件保护等功能。Trend Micro Trend Micro Serverprotect for Linux 是美国 Trend Micro 公司的一个用于企业环境的防毒软件。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞通过本地目录中放置一个恶意的 DLL 来利用，该 DLL 可以导致在安装产品期间获得管理特权，执行某些命令，修改或删除任意文件等。

CNVD 收录的相关漏洞包括：Trend Micro Security 2020 本地权限提升漏洞（CNVD-2020-73786、CNVD-2020-73785、CNVD-2020-73788）、Trend Micro InterScan Web Security Virtual Appliance 命令注入漏洞（CNVD-2020-73777、CNVD-2020-73791、CNVD-2020-73776）、Trend Micro Worry-Free Business Security 路径遍历任意远程文件删除漏洞、Trend Micro Serverprotect for Linux 缓冲区溢出漏洞。除 “Trend Micro Worry-Free Business Security 路径遍历任意远程文件删除漏洞、Trend Micro Serverprotect for Linux 缓冲区溢出漏洞”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-2020-73786

https://www.cnvd.org.cn/flaw/show/CNVD-2020-73785

https://www.cnvd.org.cn/flaw/show/CNVD-2020-73788

https://www.cnvd.org.cn/flaw/show/CNVD-2020-73777

https://www.cnvd.org.cn/flaw/show/CNVD-2020-73791

https://www.cnvd.org.cn/flaw/show/CNVD-2020-73776

https://www.cnvd.org.cn/flaw/show/CNVD-2020-73789

https://www.cnvd.org.cn/flaw/show/CNVD-2020-73784

5、TerraMaster TOS 远程代码执行漏洞

TerraMaster TOS 是为 TerraMaster 云存储 NAS 服务器开发的基于 Linux 平台的操作系统。TerraMaster TOS 4.2.06 及更早版本存在远程代码执行漏洞。攻击者可在 CSV 创建期间通过 include/makecvs.php 中的 Event 参数中的 shell 元字符利用该漏洞未经认证执行命令。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-2020-73754

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-2020-73795	D-Link DSL-2888A 操作系统命令执行漏洞	高	用户可参考如下供应商提供的安全公告获得补丁信息：https://www.dlink.com/en/products/dsl-2888a-dual-band-wireless-ac1600-gigabit-adsl2vdsl2-modem-router
CNVD-2020-73750	Dolibarr 远程代码执行漏洞（CNVD-2020-73750）	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/Dolibarr/dolibarr/releases
CNVD-2020-73168	HCL iNotes 跨站脚本漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0085892&sys_kb_id=7b149bfa1bc16098534c4159cc4bcb2c
CNVD-2020-73167	HCL Notes 授权问题漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0085913&sys_kb_id=a9185e4f1bc96498534c4159cc4bcb3a
CNVD-2020-73170	Mozilla Firefox 内存破坏代码执行漏洞	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.mozilla.org/en-US/security/advisories/mfsa2020-54/
CNVD-2020-73755	Nanosystems Supremo 访问控制错误漏洞	高	用户可参考如下供应商提供的安全公告获得补丁信息：https://www.supremocontrol.com/changelog/
CNVD-2020-	SolarWinds Orion Network	高	厂商已发布了漏洞修复程序，请及时

73323	Performance Monitor 权限许可和访问控制问题漏洞		关注更新：https://www.solarwinds.com/
CNVD-2020-73320	SolarWinds N-Central 访问控制错误漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：https://www.solarwinds.com/securityadvisory
CNVD-2020-74059	SeaCMS SQL 注入漏洞（CNVD-2020-74059）	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.seacms.net/
CNVD-2020-73166	NZXT CAM 权限许可和访问控制问题漏洞（CNVD-2020-73166）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.nzxt.com/camapp

小结：本周，IBM 产品被披露存在多个漏洞，攻击者可利用漏洞提升本地权限获取敏感信息，造成拒绝服务等。此外，Google、Microsoft、Trend Micro 等多款产品被披露存在多个漏洞，攻击者可利用漏洞获取敏感信息，造成拒绝服务，远程代码执行等。另外，TerraMaster TOS 被披露存在远程代码执行漏洞。攻击者可利用漏洞在 CSV 创建期间通过 include/makecvs.php 中的 Event 参数中的 shell 元字符未经认证执行命令。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、Mitel ShoreTel conferencing component 跨站脚本漏洞

验证描述

Mitel Connect（Mitel ShoreTel）是加拿大敏迪（Mitel）公司的一款用于办公沟通的软件。该软件可访问企业联系人、支持选择联系人开启会议、支持界面管理通话和语音邮件。

Mitel ShoreTel 19.46.1802.0 版本 conferencing component 存在跨站脚本漏洞，该漏洞源于 HOME MEETING＆页面上对时区对象的验证不足。攻击者可利用该漏洞进行反射跨站点脚本攻击(通过路径信息到 index.php)。

验证信息

POC 链接：https://www.exploit-db.com/exploits/49026

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2020-73771

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. Project Zero 团队披露微软尚未完全修复的 Windows 10 提权漏洞

存在于 Windows 系统中的一个高危漏洞，允许黑客在受感染的设备上将权限提高到内核级别。这个漏洞在今年 5 月被高级黑客作为零日漏洞使用，不过近日谷歌 Project Zero 团队使用公开的概念证明，表示这个问题依然存在，只是方法有所不同。

参考链接：https://www.cnbeta.com/articles/tech/1069915.htm

2. 工信部：已责令 1571 款违规 APP 进行整改 下架 120 款

12 月 24 日，工信部新闻发言人、信息通信发展司司长闻库在发布会上表示，工业和信息化部高度重视用户信息保护工作，持续开展移动应用程序(APP)侵害用户权益专项整治行动，截至目前，已经对 52 万款 APP 进行了技术检测工作。

参考链接：https://www.chinanews.com/cj/shipin/cns-d/2020/12-24/news876040.shtml

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