国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2021 年 04 月 26 日-2021 年 05 月 09 日　　2021 年第 17、18 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 719 个，其中高危漏洞 210 个、中危漏洞 434 个、低危漏洞 75 个。漏洞平均分值为 5.71。本周收录的漏洞中，涉及 0day 漏洞 417 个（占 58%），其中互联网上出现“PHPGurukul Online Book Store SQL 注入漏洞、Pegasystem PEGA Platform 访问控制错误漏洞”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 5288 个，与上周（2761 个）环比增加 92%。

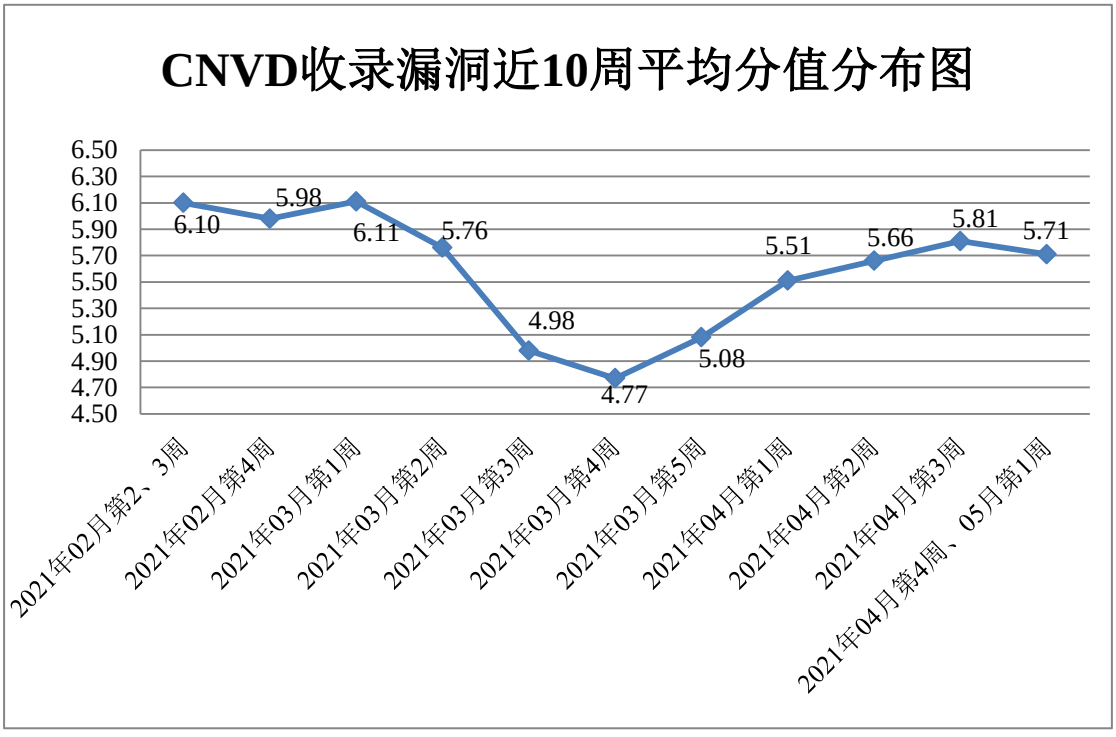

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 38 起，向基础电信企业通报漏洞事件 29 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 488 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 88 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 67 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：

淄博闪灵网络科技有限公司、珠海金山办公软件有限公司、中兴通讯股份有限公司、中兴保全股份有限公司、中消云科技股份有限公司、中科博华信息科技有限公司、中国招标公共服务平台有限公司、中国电信集团有限公司、中保无限科技有限公司、正方软件股份有限公司、镇江市云优网络科技有限公司、浙江宇视科技有限公司、浙江齐治科技股份有限公司、浙江兰德纵横网络技术股份有限公司、浙江大华技术股份有限公司、长沙友点软件科技有限公司、漳州市芗城帝兴软件开发有限公司、友讯电子设备（上海）有限公司、优酷信息技术（北京）有限公司、优刻得科技股份有限公司、用友网络科技股份有限公司、医惠科技有限公司、讯全信息科技(上海)有限公司、西安众邦网络科技有限公司、西安大西信息科技有限公司、西安奥枫软件有限公司、无锡线上线下通讯信息技术股份有限公司、纬衡浩建科技（深圳）有限公司、网际傲游（北京）科技有限公司、统信软件技术有限公司、太原易思软件技术有限公司、台达电子企业管理（上海）有限公司、苏州科达科技股份有限公司、松下电器（中国）有限公司、泗洪雷速软件有限公司、四平市九州易通科技有限公司、四川卓迈科技有限公司、深圳市智物联网络有限公司、深圳市智博通电子有限公司、深圳市优特普技术有限公司、深圳市易宇通科技有限公司、深圳市迅雷网络技术有限公司、深圳市信锐网科技术有限公司、深圳市西迪特科技有限公司、深圳市微客互动有限公司、深圳市网心科技有限公司、深圳市腾狐物联科技有限公司、深圳市六合未来科技有限公司、深圳市磊科实业有限公司、深圳市锟铻科技有限公司、深圳市看护家科技有限公司、深圳市简芯科技有限公司、深圳市吉祥腾达科技有限公司、深圳市宏电技术股份有限公司、深圳市河辰通讯技术有限公司、深圳市鼎游信息技术有限公司、深圳市触拓科技有限公司、深圳市朝恒辉网络科技有限公司、上海中消网络科技有限公司、上海小蚁科技有限公司、上海罗湖斯自动化技术有限公司、上海建文软件科技有限公司、上海汇招信息技术有限公司、上海孚盟软件有限公司、上海斐讯数据通信技术有限公司、上海泛微网络科技股份有限公司、上海二三四五网络控股集团股份有限公司、上海楚果信息技术有限公司、上海博达数据通信有限公司、上海艾泰科技有限公司、陕西德森特软件有限公司、山东国子软件股份有限公司、厦门昕桐科技有限公司、厦门四信通信科技有限公司、厦门市灵鹿谷科技有限公司、润申信息科技（上海）有限公司、锐捷网络股份有限公司、任丘市正中网络科技有限公司、全讯汇聚网络科技（北京）有限公司、奇安信科技集团股份有限公司、普联技术有限公司、

南京苏文软件技术有限公司、南昌蓝智科技有限公司、迈普通信技术股份有限公司、凌锐蓝信科技（北京）有限公司、廊坊市极致网络科技有限公司、莱克斯科技（北京）有限公司、飓风(深圳)软件有限公司、金蝶软件（中国）有限公司、江苏易索电子科技股份有限公司、江苏易安联网络技术有限公司、嘉兴想天信息科技有限公司、慧与（中国）有限公司、惠普贸易（上海）有限公司、湖南翱云网络科技有限公司、河北南昊高新技术开发有限公司、合肥晨光电子科技有限公司、杭州新中大科技股份有限公司、杭州可道云网络有限公司、杭州海康威视系统技术有限公司、杭州海康威视数字技术股份有限公司、杭州安恒信息技术股份有限公司、杭州艾朴软件有限公司、哈尔滨新中新电子股份有限公司、国泰新点软件股份有限公司、广州图创计算机软件开发有限公司、广州数易信息技术有限公司、广州市溢信科技股份有限公司、广州齐博网络科技有限公司、广州红帆科技有限公司、广州海鹚网络科技有限公司、广州安网通信技术有限公司、广联达科技股份有限公司、富士胶片（中国）投资有限公司、福建四创软件有限公司、福建升腾资讯有限公司、帆软软件有限公司、东莞市通天星软件科技有限公司、戴尔(中国)有限公司、成都友加畅捷科技有限公司、成都瑞科公司、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、博世（中国）投资有限公司、北京中科商信科技有限公司、北京中科商软软件有限公司、北京中成科信科技发展有限公司、北京致远互联软件股份有限公司、北京亿中邮信息技术有限公司、北京文网亿联科技有限公司、北京网康科技有限公司、北京万维捷通软件技术有限公司、北京万户网络技术有限公司、北京通达志成科技有限公司、北京硕人时代科技股份有限公司、北京世纪长秋科技有限公司、北京时空智友科技有限公司、北京神州数码云科信息技术有限公司、北京山石网科信息技术有限公司、北京瑞星网安技术股份有限公司、北京清流技术股份有限公司、北京猎鹰安全科技有限公司、北京库巴扎信息科技有限公司、北京金和网络股份有限公司、北京汉柏科技有限公司、北京国炬信息技术有限公司、北京辰信领创信息技术有限公司、北京北大方正电子有限公司、北京百卓网络技术有限公司、北京安博通科技股份有限公司、北大医疗信息技术有限公司、傲拓科技股份有限公司、安科瑞电气股份有限公司、安徽辛普科技有限公司、安徽科迅教育装备集团有限公司、阿里巴巴集团安全应急响应中心、合肥晨光科技、河北欧润天腾云梦吧网络工作室、熊海 CMS、若依 CMS、英飞拓（Infinova）、梦想 CMS、海洋 CMS、zzzcms、XHCMS、UCMS、TRENDnet、The Apache Software Foundation、Textpattern CMS、SEMCMS、PublicCMS、PowerJob、Oracle、MOBOTIX、MiniCMS、Lexmark、Kollmorgen、Geovision、Catfish CMS、Axis Communications、Adobe、ABBYY 和 115CMS。

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、远江盛邦（北

京）网络安全科技股份有限公司、北京神州绿盟科技有限公司、哈尔滨安天科技集团股份有限公司、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。杭州海康威视数字技术股份有限公司、北京华顺信安科技有限公司、北京山石网科信息技术有限公司、河南信安世纪科技有限公司、中国电信股份有限公司网络安全产品运营中心、山东新潮信息技术有限公司、河南灵创电子科技有限公司 、新疆海狼科技有限公司、北京天地和兴科技有限公司、武汉明嘉信信息安全检测评估有限公司、安徽长泰信息安全服务有限公司、杭州迪普科技股份有限公司、北京顶象技术有限公司、西安交大捷普网络科技有限公司、山东泽鹿安全技术有限公司、江苏保旺达软件技术有限公司、日照天鉴网络科技有限公司、小安（北京）科技有限公司、北京安帝科技有限公司、北京圣博润高新技术股份有限公司、杭州木链物联网科技有限公司、京东云安全、北京墨云科技有限公司、广州安亿信软件科技有限公司、深圳市魔方安全科技有限公司、北京君云天下科技有限公司、海南神州希望网路有限公司、上海纽盾科技股份有限公司、武汉安域信息安全技术有限公司、浙江御安信息技术有限公司、北京机沃科技有限公司、北京信联科汇科技有限公司、博雅正链（北京）科技有限公司、博智安全科技股份有限公司、贵州多彩宝互联网服务有限公司、国网山东省电力公司、杭州乒乓智能技术股份有限公司、清远职业技术学院、上海市信息安全测评认证中心、上海崤函信息科技有限公司、上海心河信息技术有限公司、重庆贝特计算机系统工程有限公司及其他个人白帽子向CNVD提交了5288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2486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）	1035	1035
斗象科技（漏洞盒子）	771	771
上海交大	680	680
北京天融信网络安全技术有限公司	548	7
远江盛邦（北京）网络安全科技股份有限公司	429	429
北京神州绿盟科技有限公司	292	8
哈尔滨安天科技集团股份有限公司	258	0
深信服科技股份有限公司	202	0
新华三技术有限公司	198	0
华为技术有限公司	171	0

北京数字观星科技有限公司	160	0
恒安嘉新（北京）科技股份公司	123	0
卫士通信息产业股份有限公司	86	0
国瑞数码零点实验室	70	0
北京启明星辰信息安全技术有限公司	62	1
西安四叶草信息技术有限公司	33	33
内蒙古奥创科技有限公司	14	14
中国电信集团系统集成有限责任公司	12	12
北京知道创宇信息技术股份有限公司	8	0
北京奇虎科技有限公司	6	6
北京智游网安科技有限公司	1	1
杭州安恒信息技术股份有限公司	1	1
南京联成科技发展股份有限公司	1	1
杭州海康威视数字技术股份有限公司	343	343
北京华顺信安科技有限公司	200	0
北京山石网科信息技术有限公司	127	127
河南信安世纪科技有限公司	124	124
中国电信股份有限公司网络安全产品运营中心	76	36
山东新潮信息技术有限公司	55	55
河南灵创电子科技有限公司	45	45
新疆海狼科技有限公司	44	44

北京天地和兴科技有限公司	40	40
武汉明嘉信信息安全检测评估有限公司	35	35
安徽长泰信息安全服务有限公司	15	15
杭州迪普科技股份有限公司	13	0
北京顶象技术有限公司	10	10
西安交大捷普网络科技有限公司	10	10
山东泽鹿安全技术有限公司	10	10
江苏保旺达软件技术有限公司	9	9
日照天鋆网络科技有限公司	9	9
小安（北京）科技有限公司	9	9
北京安帝科技有限公司	8	8
北京圣博润高新技术股份有限公司	8	8
杭州木链物联网科技有限公司	8	8
京东云安全	4	4
北京墨云科技有限公司	3	3
广州安亿信软件科技有限公司	3	3
深圳市魔方安全科技有限公司	3	3
北京君云天下科技有限公司	2	2
海南神州希望网路有限公司	2	2
上海纽盾科技股份有限公司	2	2
武汉安域信息安全技术有限公司	2	2
浙江御安信息技术有	2	2

限公司		
北京机沃科技有限公司	2	2
北京信联科汇科技有限公司	1	1
博雅正链（北京）科技有限公司	1	1
博智安全科技股份有限公司	1	1
贵州多彩宝互联网服务有限公司	1	1
国网山东省电力公司	1	1
杭州乒乓智能技术股份有限公司	1	1
清远职业技术学院	1	1
上海市信息安全测评认证中心	1	1
上海崤函信息科技有限公司	1	1
上海心河信息技术有限公司	1	1
重庆贝特计算机系统工程有限公司	1	1
CNCERT 宁夏分中心	13	13
CNCERT 西藏分中心	8	8
CNCERT 山西分中心	7	7
CNCERT 天津分中心	5	5
CNCERT 浙江分中心	5	5
CNCERT 湖南分中心	2	2
CNCERT 青海分中心	2	2
CNCERT 贵州分中心	1	1
CNCERT 山东分中心	1	1
个人	1264	1264
报送总计	7703	5288

本周漏洞按类型和厂商统计

本周，CNVD 收录了 719 个漏洞。应用程序 298 个，WEB 应用 207 个，网络设备（交换机、路由器等网络端设备）106 个，数据库 36 个，操作系统 33 个，安全产品 32 个，智能设备（物联网终端设备）7 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	298
WEB 应用	207
网络设备（交换机、路由器等网络端设备）	106
数据库	36
操作系统	33
安全产品	32
智能设备（物联网终端设备）	7

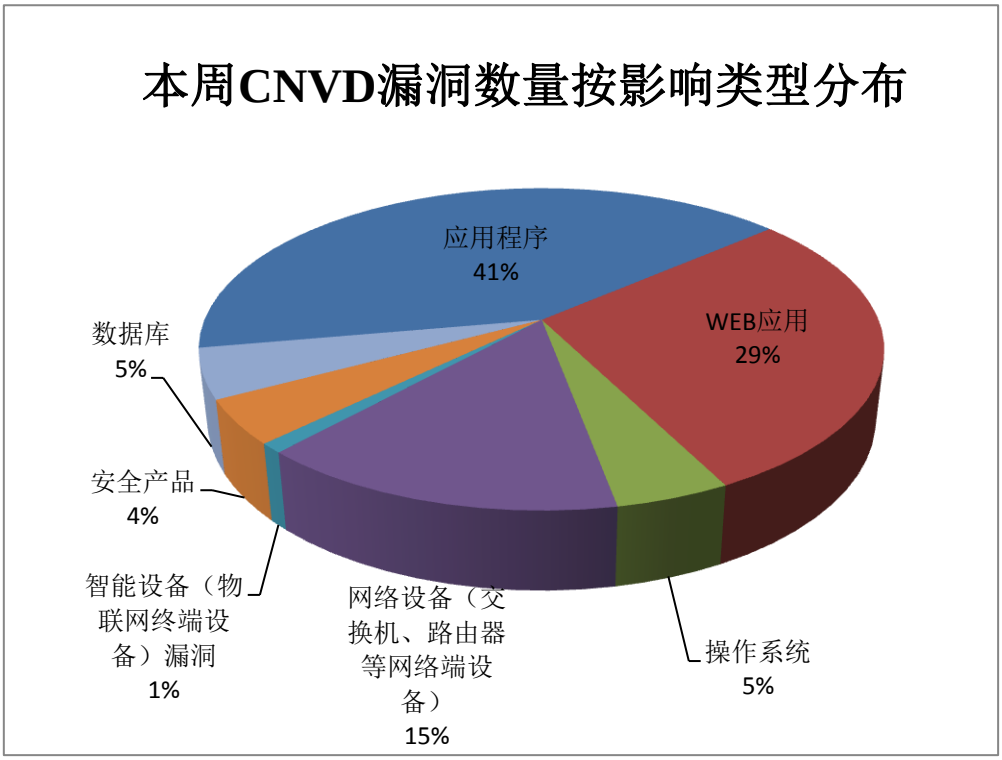

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Oracle、锐捷网络股份有限公司、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	Oracle	45	6%
2	锐捷网络股份有限公司	34	5%
3	IBM	27	4%
4	Google	24	3%
5	Mozilla	19	3%
6	深圳市吉祥腾达科技有限公司	17	2%
7	深信服科技股份有限公司	16	2%
8	Microsoft	14	2%

9	NLnet Labs	12	2%
10	其他	511	71%

本周行业漏洞收录情况

本周，CNVD 收录了 112 个电信行业漏洞，19 个移动互联网行业漏洞，24 个工控行业漏洞（如下图所示）。其中，“Motorola MH702 信任管理问题漏洞、Oracle MySQL Server 输入验证错误漏洞（CNVD-2021-30889）、Google Android 授权问题漏洞（CNVD-2021-31238）、Schneider Electric PowerLogic 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/

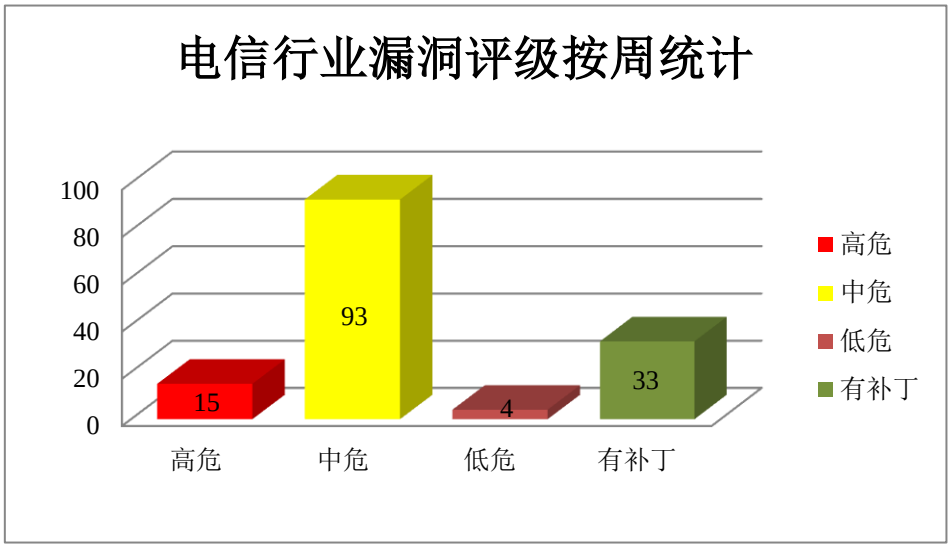

图 3 电信行业漏洞统计

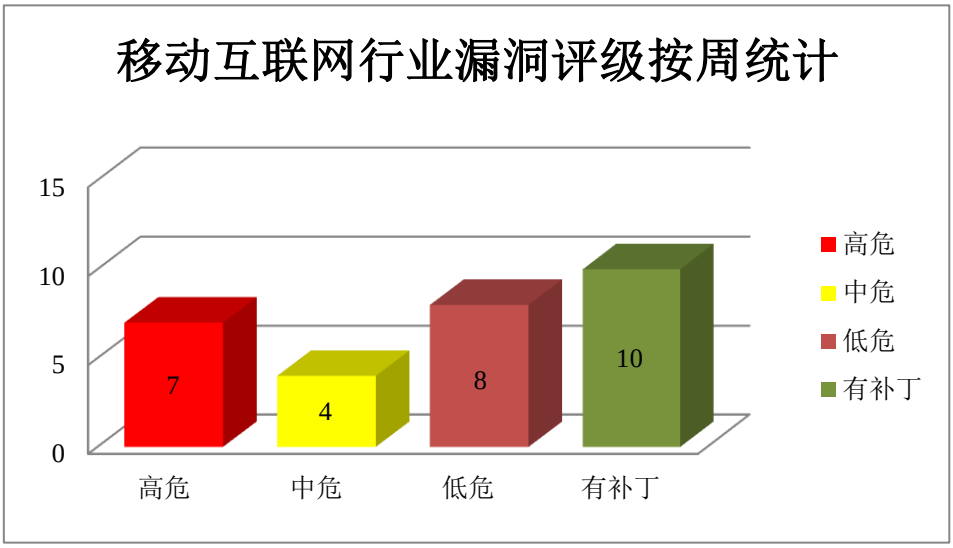

图 4 移动互联网行业漏洞统计

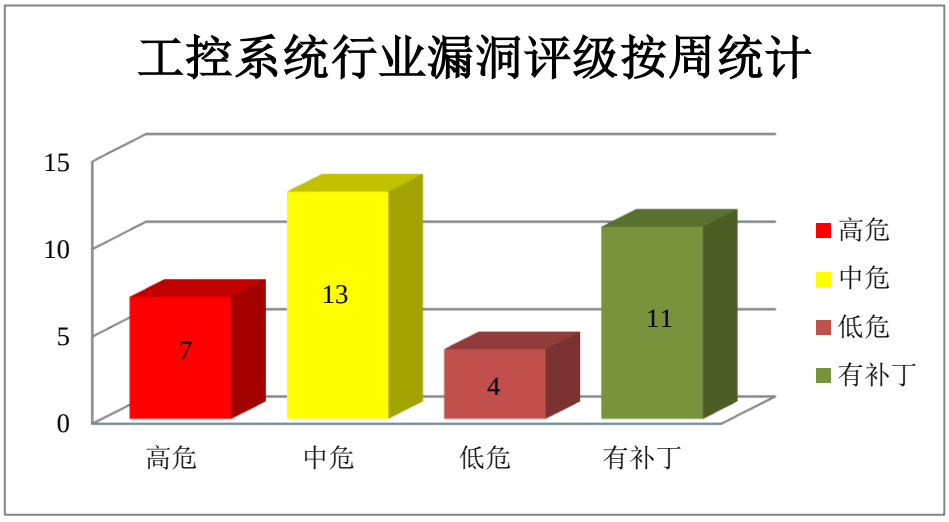

图 5 工控系统行业漏洞统计

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、Oracle 产品安全漏洞

Oracle MySQL Server 是美国甲骨文（Oracle）公司的一款关系型数据库。本周，上述产品被披露存在输入验证错误漏洞，攻击者可利用漏洞导致 MySQL 服务器挂起或频繁重复发生崩溃（完整的 DOS）。

CNVD 收录的相关漏洞包括：Oracle MySQL Server 输入验证错误漏洞（CNVD-2021-30889、CNVD-2021-30923、CNVD-2021-30922、CNVD-2021-30921、CNVD-2021-30920、CNVD-2021-30926、CNVD-2021-30925、CNVD-2021-30924）。其中，“Oracle MySQL Server 输入验证错误漏洞（CNVD-2021-30889）”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-2021-30889

https://www.cnvd.org.cn/flaw/show/CNVD-2021-30923

https://www.cnvd.org.cn/flaw/show/CNVD-2021-30922

https://www.cnvd.org.cn/flaw/show/CNVD-2021-30921

https://www.cnvd.org.cn/flaw/show/CNVD-2021-30920

https://www.cnvd.org.cn/flaw/show/CNVD-2021-30926

https://www.cnvd.org.cn/flaw/show/CNVD-2021-30925

https://www.cnvd.org.cn/flaw/show/CNVD-2021-30924

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 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。Windows Error Reporting（WER）是其中的一个错误报告组件。Microsoft Windows Runtime（.net framework）是美国微软（Microsoft）公司的一款 Windows 操作系统中必要的功能支持库。Windows Installer 是其中的一个基于 Windows 系统的工具组件，主要用于管理和配置软件服务。Windows Kernel 是其中的一个 Windows 系统内核。Windows Text Service Framework（TSF）是其中的一个文本服务框架。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞在用户系统上运行特制的应用程序利用该漏洞以提升的权限执行任意代码，进而安装程序，查看、更改或删除数据或者创建具有全部用户权限的新帐户。

CNVD 收录的相关漏洞包括：Microsoft Windows Runtime 权限提升漏洞（CNVD-2021-31217、CNVD-2021-31215、CNVD-2021-31219）、Microsoft Windows Error Reporting 权限提升漏洞（CNVD-2021-31216）、Microsoft Windows Feedback Hub 权限提升漏洞、Microsoft Windows Installer 权限提升漏洞（CNVD-2021-31220）、Microsoft Windows Kernel 权限提升漏洞（CNVD-2021-31218）、Microsoft Windows TSF 权限提升漏洞。其中“Microsoft Windows Feedback Hub 权限提升漏洞”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-2021-31217
https://www.cnvd.org.cn/flaw/show/CNVD-2021-31216
https://www.cnvd.org.cn/flaw/show/CNVD-2021-31215
https://www.cnvd.org.cn/flaw/show/CNVD-2021-31214
https://www.cnvd.org.cn/flaw/show/CNVD-2021-31220
https://www.cnvd.org.cn/flaw/show/CNVD-2021-31219
https://www.cnvd.org.cn/flaw/show/CNVD-2021-31218
https://www.cnvd.org.cn/flaw/show/CNVD-2021-31222

3、Google 产品安全漏洞

Google Chrome 是美国谷歌（Google）公司的一款 Web 浏览器。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞破坏脆弱的系统，可以创建一个特制的网页，诱使受害者访问该网页，触发释放后使用错误并在目标系统上执行任意代码。

CNVD 收录的相关漏洞包括：Google Chrome 资源管理错误漏洞（CNVD-2021-31247、CNVD-2021-31246、CNVD-2021-31239）、Google Chrome 输入验证错误漏洞（CNVD-2021-31242）、Google Chrome 释放后重用漏洞（CNVD-2021-31251、CNVD-2021-31250）、Google Chrome 类型混淆漏洞（CNVD-2021-31241）、Google Chrome 缓冲区溢出漏洞（CNVD-2021-31240）。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-2021-31247

https://www.cnvd.org.cn/flaw/show/CNVD-2021-31246

https://www.cnvd.org.cn/flaw/show/CNVD-2021-31239

https://www.cnvd.org.cn/flaw/show/CNVD-2021-31242

https://www.cnvd.org.cn/flaw/show/CNVD-2021-31251

https://www.cnvd.org.cn/flaw/show/CNVD-2021-31250

https://www.cnvd.org.cn/flaw/show/CNVD-2021-31241

https://www.cnvd.org.cn/flaw/show/CNVD-2021-31240

4、Schneider Electric 产品安全漏洞

Schneider Electric PowerLogic 是法国施耐德电气（Schneider Electric）公司的一个工控设备。提供提高功率因数来提高电源质量，排除电源故障，从而保护网络、装置和操作员。Schneider Electric Interactive Graphical SCADA System（IGSS）是法国施耐德电气（Schneider Electric）公司的一套用于监控和控制工业过程的 SCADA（数据采集与监控系统）系统。Schneider Electric C-Bus Toolkit 是法国施耐德电气（Schneider Electric）公司的一款应用程序。用于在个人计算机上运行，配置和调试 C-Bus 的安装。Schneider Electric EcoStruxure Control Expert（前称 Unity Pro）是法国施耐德电气（Schneider Electric）公司的一套用于 Schneider Electric 逻辑控制器产品的编程软件。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞发送特制的 TCP 数据包利用该漏洞导致仪表重启或远程代码执行，导入恶意 CGF（配置组文件）利用该漏洞导致任意读取和写入。

CNVD 收录的相关漏洞包括：Schneider Electric PowerLogic 缓冲区溢出漏洞、Schneider Electric Interactive Graphical SCADA System 缓冲区溢出漏洞（CNVD-2021-31178、CNVD-2021-31177）、Schneider Electric C-Bus Toolkit 路径遍历漏洞（CNVD-2021-31171、CNVD-2021-31170、CNVD-2021-31172）、Schneider Electric EcoStruxure Control Expert PLC 拒绝服务漏洞、Schneider Electric C-Bus Toolkit 权限许可和访问控制问题漏洞。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-2021-31176

https://www.cnvd.org.cn/flaw/show/CNVD-2021-31178

https://www.cnvd.org.cn/flaw/show/CNVD-2021-31177

https://www.cnvd.org.cn/flaw/show/CNVD-2021-31171

https://www.cnvd.org.cn/flaw/show/CNVD-2021-31183

https://www.cnvd.org.cn/flaw/show/CNVD-2021-31173

https://www.cnvd.org.cn/flaw/show/CNVD-2021-31170

https://www.cnvd.org.cn/flaw/show/CNVD-2021-31172

5、Pegasystem PEGA Platform 访问控制错误漏洞

Pegasystem PEGA Platform 是英国 Pegasystem 公司的一套应用程序开发平台。该平台用于开发 BPM（业务流程管理）、案例管理、实时决策和 CRM（客户关系管理）等应用程序。本周，Pegasystem PEGA Platform 被披露存在访问控制错误漏洞。攻击者可可通过=GetWebInfo 利用该漏洞获取敏感信息。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-2021-31919

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-2021-31930	Zoho Corporation Manage Engine OpManager 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.manageengine.com/network-monitoring/
CNVD-2021-31474	Xiaomi Mi Jia ink-jet printer 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://privacy.mi.com/trust#/security/vulnerability-management/vulnerability-announcement/detail?id=13
CNVD-2021-32035	Wowza Media Systems Streaming Engine 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://www.wowza.com/docs/wowza-streaming-engine-4-8-5-release-notes
CNVD-2021-31925	Webmin 输入验证错误漏洞	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/webmin/webmin/commit/1163f3a7f418f249af64890f4636575e687e9de7#diff-9b33fd8f5603d4f0d1428689bc36f24af4770608a22c0d92b7a8bcc522450dc6
CNVD-2021-31932	VMware vRealize Operations 任意文件写入漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://www.vmware.com/security/advisories/VMSA-2021-0004.html
CNVD-2021-32027	Tobesoft Xplatform 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：http://www.nexacro.com/product/Xplatf

			orm.do
CNVD-2021-33043	SolarWinds Orion Platform 路径遍历漏洞（CNVD-2021-33043）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.zerodayinitiative.com/advisories/ZDI-21-067/
CNVD-2021-31176	Schneider Electric PowerLogic 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://www.se.com/ww/en/download/document/SEVD-2021-068-02
CNVD-2021-31235	Rapid7 Metasploit Framework 代码问题漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://help.rapid7.com/metasploit/release-notes/archive/2020/10/
CNVD-2021-31949	Qnap Systems QNAP HBS 3 授权问题漏洞	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://www.qnap.com/en/security-advisory/QSA-21-13

小结：本周，Oracle 产品被披露存在多个漏洞，攻击者可利用漏洞导致 MySQL 服务器挂起或频繁重复发生崩溃（完整的 DOS）。此外，Microsoft、Google、Schneider Electric 等多款产品被披露存在多个漏洞，攻击者可利用漏洞在用户系统上运行特制的应用程序利用该漏洞以提升的权限执行任意代码，进而安装程序，查看、更改或删除数据或者创建具有全部用户权限的新帐户，发送特制的 TCP 数据包导致仪表重启或远程代码执行，导入恶意 CGF（配置组文件）导致任意读取和写入等。另外，Pegasystem PEGA Platform 被披露存在访问控制错误漏洞。攻击者可通过=GetWebInfo 利用漏洞获取敏感信息。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、Remote Clinic 跨站脚本漏洞（CNVD-2021-31665）

验证描述

Remote Clinic 是一款开源诊所管理系统，可让您通过 Web 远程管理您的诊所。

Remote Clinic v2.0 版本中的/medicines 存在存储型跨站脚本漏洞。攻击者可通过 Medicine Name 字段利用该漏洞进行跨站脚本攻击。

验证信息

POC 链接：https://github.com/remoteclinic/RemoteClinic/issues/14

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2021-31665

信息提供者

华为技术有限公司

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. 思科修复了允许创建管理账户，以 root 身份执行命令的漏洞

思科修复了 SD-WAN vManage 和 HyperFlex HX 软件的关键漏洞，这些漏洞可能允许创建管理账户，并以 root 身份执行命令。

参考链接：https://securityaffairs.co/wordpress/117560/security/cisco-sd-wan-vmanage-hyperflex-hx-flaws.html

2. VMware 修复了 vRealize Business for Cloud 中的关键 RCE 错误

VMware 发布了安全更新，以解决 vRealize Business for Cloud 中的一个严重漏洞，该漏洞使未经认证的攻击者可以在有漏洞的服务器上远程执行恶意代码。

参考链接：https://www.bleepingcomputer.com/news/security/vmware-fixes-critical-rce-bug-in-vrealize-business-for-cloud/

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