国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2021 年 08 月 02 日-2021 年 08 月 08 日　　2021 年第 31 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 413 个，其中高危漏洞 106 个、中危漏洞 247 个、低危漏洞 60 个。漏洞平均分值为 5.58。本周收录的漏洞中，涉及 0day 漏洞 248 个（占 60%），其中互联网上出现“MetInfo SQL 注入漏洞（CNVD-2021-59068）、HuCart 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 3796 个，与上周（4935 个）环比减少 23%。

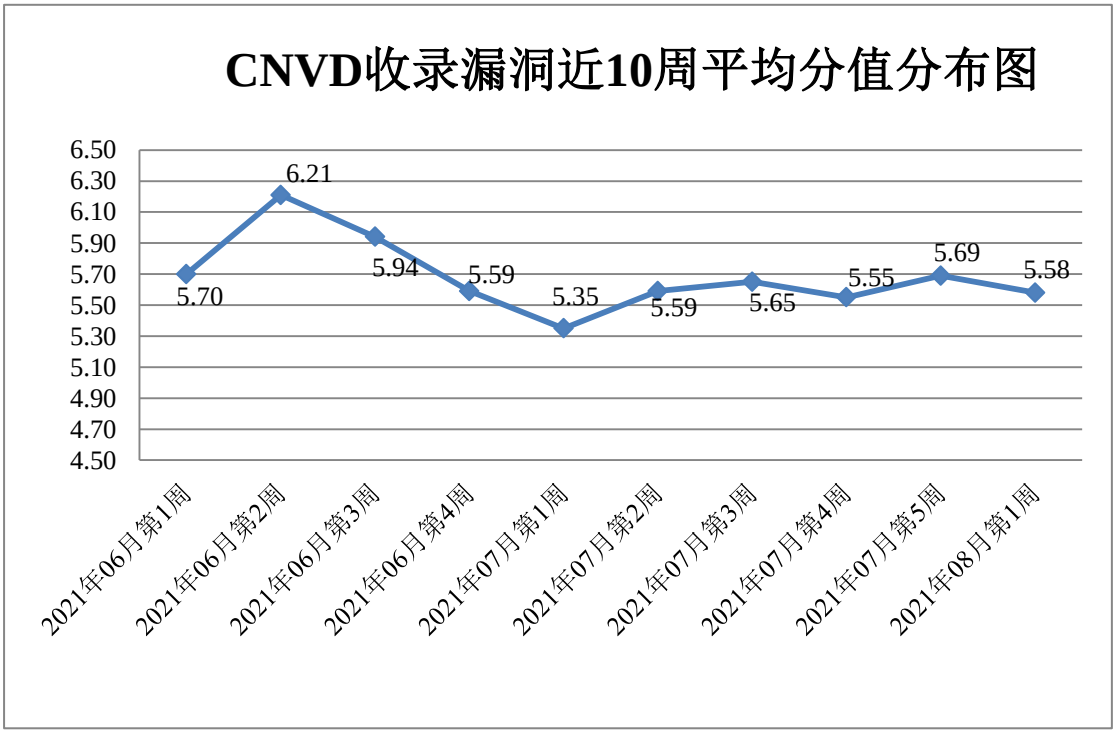

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 24 起，向基础电信企业通报漏洞事件 33 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 357 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 49 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 42 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：

紫光软件系统有限公司、淄博闪灵网络科技有限公司、珠海新华通软件股份有限公司、珠海玖时光科技有限公司、众勤通信设备贸易（上海）有限公司、中兴通讯股份有限公司、中建一局集团第一建筑有限公司、中海地产集团有限公司、中国建筑第八工程局有限公司、中国大唐集团公司、中国船舶集团有限公司、郑州明网信息技术有限公司、浙江宇视科技有限公司、张家港鼎力科技有限公司、友讯电子设备（上海）有限公司、用友网络科技股份有限公司、研华科技（中国）有限公司、徐州亿优网架钢结构工程有限公司、西安捷达测控有限公司、武汉爱码农网络科技有限公司、微软（中国）有限公司、天信仪表集团有限公司、天津创享信息科技有限公司、宿迁鑫潮信息技术有限公司、苏州科达科技股份有限公司、松下电器（中国）有限公司、四创科技有限公司、思科系统（中国）网络技术有限公司、世邦通信股份有限公司、施耐德电气（中国）有限公司、深圳市微控一指通科技有限公司、深圳市吉祥腾达科技有限公司、深圳警翼智能科技股份有限公司、上海纵之格科技有限公司、上海卓卓网络科技有限公司、上海旋荣科技股份有限公司、上海建文软件科技有限公司、上海鸿仕网络科技有限公司、上海碧海网络科技有限公司、厦门亿联网络技术股份有限公司、厦门四信通信科技有限公司、润申信息科技（上海）有限公司、青岛通软网络科技有限公司、迈普通信技术股份有限公司、乐山全新媒体科技发展有限公司、江西铭软科技有限公司、江苏固德威电源科技股份有限公司、嘉兴想天信息科技有限公司、吉翁电子（深圳）有限公司、惠普贸易（上海）有限公司、华信数安(深圳)技术有限公司、华特数字科技有限公司、湖南随心所想网络科技有限公司、湖南建研信息技术股份有限公司、合肥启凡网络科技有限公司、杭州雄迈信息技术有限公司、杭州吉拉科技有限公司、桂林崇胜网络科技有限公司、广州众米信息科技有限公司、广州天呈网络技术有限公司、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、富士胶片商业创新（中国）有限公司、福建福昕软件开发股份有限公司、大唐电信科技股份有限公司、成都星锐蓝海网络科技有限公司、成都飞鱼星科技股份有限公司、郴州帝云网络科技有限公司、北京中体联合数据科技有限公司、北京中创视讯科技有限公司、北京云帆互联科技有限公司、北京夜猫天诚网络科技有限公司、北京星网锐捷网络技术有限公司、北京新盛阳光科技有限公司、北京小象智慧科技有限公司、北京万讯博通科技发展有限公司、北京万维盈创科技发展有限公司、北京通达信科科技有限公司、北京市商汤科技开发有限公司、北京神州数码云科信息技术有限

公司、北京恰维网络科技有限公司、北京米尔伟业科技有限公司、北京猎鹰安全科技有限公司、北京酷我科技有限公司、北京金和网络股份有限公司、北京火木科技有限公司、北京邦永科技有限公司、北京百卓网络技术有限公司、包头市助友科技有限公司、安徽建工集团控股有限公司、爱普生（中国）有限公司、阿帕数字技术有限公司、阿里巴巴集团安全应急响应中心、百度安全应急响应中心、中保科技集團、智睿软件、成都零起飞网络、海洋 CMS、YzmCMS、Victor Alagwu、TOTOLINK、SEMCMS、santesoft、OneBlog、Nitro 、 NETGEAR 、 malun 、 HuCart 、 FINECMS 、 CourseSEL 、 BEESCMS 、 Axis Communications AB、AKCMS 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、厦门服云信息科技有限公司、新华三技术有限公司、北京启明星辰信息安全技术有限公司等单位报送公开收集的漏洞数量较多。北京信联科汇科技有限公司、山东云天安全技术有限公司、北京山石网科信息技术有限公司、京东云安全、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、浙江木链物联网科技有限公司、南京众智维信息科技有限公司、山东新潮信息技术有限公司、山东泽鹿安全技术有限公司、河南灵创电子科技有限公司 、广东蓝爵网络安全技术股份有限公司、安徽长泰信息安全服务有限公司、北京安帝科技有限公司、北京天地和兴科技有限公司、重庆都会信息科技、河南信安世纪科技有限公司、杭州迪普科技股份有限公司、上海纽盾科技股份有限公司、广西等保安全测评有限公司、北京云科安信科技有限公司（Seraph 安全实验室）、南京树安信息技术有限公司、北京远禾科技有限公司、广州安亿信软件科技有限公司、北京云弈科技有限公司、上海市信息安全测评认证中心、武汉明嘉信信息安全检测评估有限公司、西藏熙安信息技术有限责任公司、广州乐轩玄彩电子科技有限公司、江苏快页信息技术有限公司、南方电网数字电网研究院有限公司、星云博创科技有限公司、四川赛虎科技有限公司、浙江乾冠信息安全研究院、浙江御安信息技术有限公司、阿里巴巴网络技术有限公司及其他个人白帽子向 CNVD 提交了 3796 个以事件型漏洞为主的原创漏洞，其中包括斗象科技（漏洞盒子）、上海交大和奇安信网神（补天平台）向 CNVD 共享的白帽子报送的 1265 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）	603	603
斗象科技（漏洞盒子）	454	454

北京神州绿盟科技有限公司	392	9
哈尔滨安天科技集团股份有限公司	259	0
厦门服云信息科技有限公司	253	2
上海交大	208	208
新华三技术有限公司	177	0
北京启明星辰信息安全技术有限公司	125	70
恒安嘉新（北京）科技股份公司	120	0
北京数字观星科技有限公司	110	1
华为技术有限公司	108	0
国瑞数码零点实验室	60	0
深信服科技股份有限公司	43	0
北京天融信网络安全技术有限公司	22	22
南京联成科技发展股份有限公司	21	21
北京安信天行科技有限公司	18	18
内蒙古奥创科技有限公司	9	9
浙江大华技术股份有	7	7

限公司		
北京知道创宇信息技术股份有限公司	2	0
北京信联科汇科技有限公司	324	324
山东云天安全技术有限公司	216	216
北京山石网科信息技术有限公司	179	179
联想全球安全实验室	177	0
京东云安全	120	120
北京华云安信息技术有限公司	105	105
杭州海康威视数字技术股份有限公司	88	88
浙江木链物联网科技有限公司	78	78
南京众智维信息科技有限公司	69	69
山东新潮信息技术有限公司	52	52
山东泽鹿安全技术有限公司	46	46
河南灵创电子科技有限公司	44	44
广东蓝爵网络安全技术股份有限公司	36	36
安徽长泰信息安全服务有限公司	31	31
北京安帝科技有限公司	21	21

中国电信股份有限公司网络安全产品运营中心	20	0
北京天地和兴科技有限公司	19	19
重庆都会信息科技	19	19
河南信安世纪科技有限公司	15	15
杭州迪普科技股份有限公司	15	1
上海纽盾科技股份有限公司	14	14
广西等保安全测评有限公司	8	8
北京云科安信科技有限公司（Seraph 安全实验室）	6	6
南京树安信息技术有限公司	6	6
北京远禾科技有限公司	5	5
广州安亿信软件科技有限公司	3	3
西门子（中国）有限公司	4	0
北京云弈科技有限公司	2	2
上海市信息安全测评认证中心	2	2
武汉明嘉信信息安全检测评估有限公司	2	2
西藏熙安信息技术有限责任公司	2	2

广州乐轩玄彩电子科技有限公司	1	1
江苏快页信息技术有限公司	1	1
南方电网数字电网研究院有限公司	1	1
星云博创科技有限公司	1	1
四川赛虎科技有限公司	1	1
浙江乾冠信息安全研究院	1	1
浙江御安信息技术有限公司	1	1
阿里巴巴网络技术有限公司	1	1
CNCERT 四川分中心	6	6
CNCERT 西藏分中心	5	5
CNCERT 山东分中心	4	4
CNCERT 贵州分中心	2	2
CNCERT 河北分中心	1	1
CNCERT 青海分中心	1	1
个人	832	832
报送总计	5578	3796

本周漏洞按类型和厂商统计

本周，CNVD 收录了 413 个漏洞。WEB 应用 166 个，应用程序 155 个，网络设备（交换机、路由器等网络端设备）56 个，操作系统 15 个，智能设备（物联网终端设备）10 个，安全产品 10 个，数据库 1 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
WEB 应用	166
应用程序	155
网络设备（交换机、路由器等网络端设备）	56
操作系统	15

智能设备（物联网终端设备）	10
安全产品	10
数据库	1

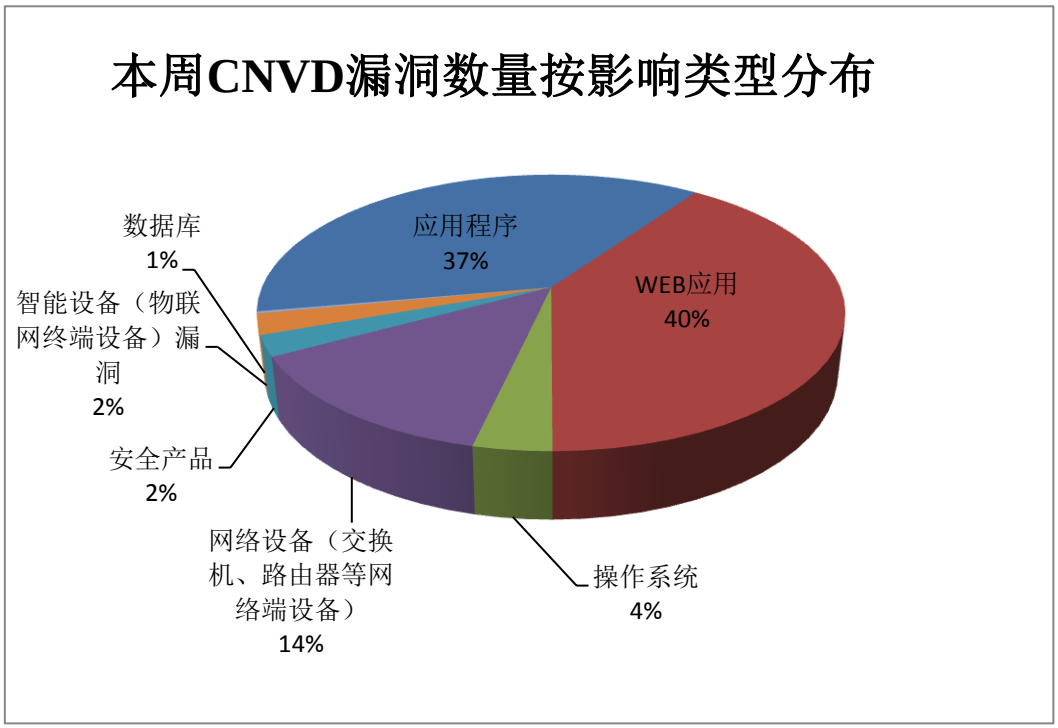

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Oracle、NETGEAR、Foxit 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	16	4%
2	NETGEAR	15	4%
3	Foxit	11	3%
4	HCC Embedded	10	2%
5	Microsoft	10	2%
6	Accusoft	9	2%
7	Acronis	8	2%
8	Apport	8	2%
9	Envoy	8	2%
10	其他	318	77%

本周行业漏洞收录情况

本周，CNVD 收录了 31 个电信行业漏洞，20 个移动互联网行业漏洞，12 个工控行

业漏洞（如下图所示）。其中，“Advantech WebAccess/SCADA 缓冲区溢出漏洞（CNVD-2021-59234）、Advantech WebAccess/SCADA 路径遍历漏洞（CNVD-2021-59235）”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/

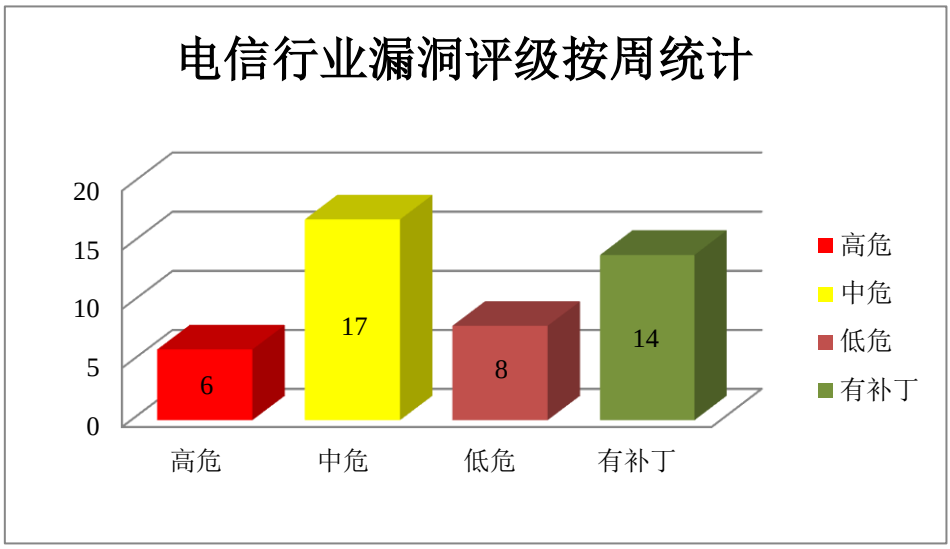

图 3 电信行业漏洞统计

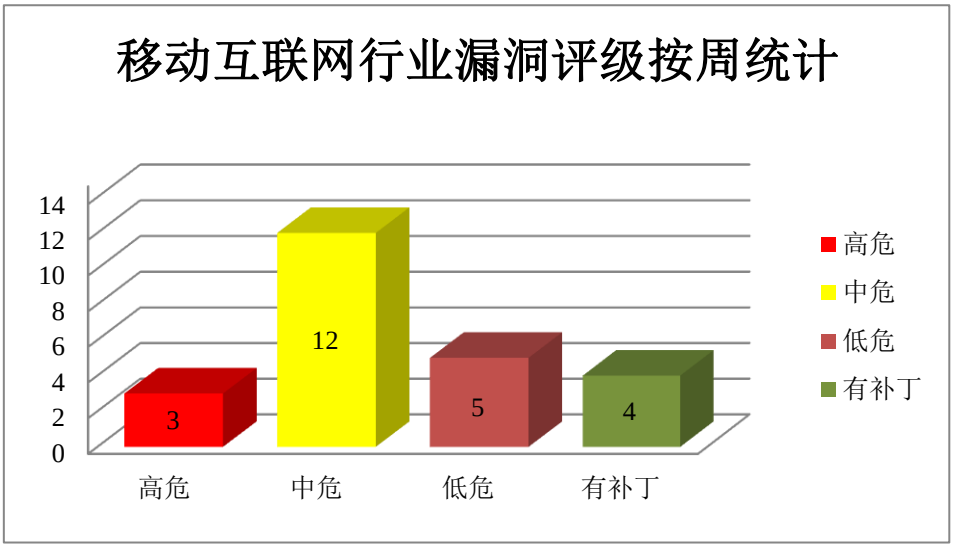

图 4 移动互联网行业漏洞统计

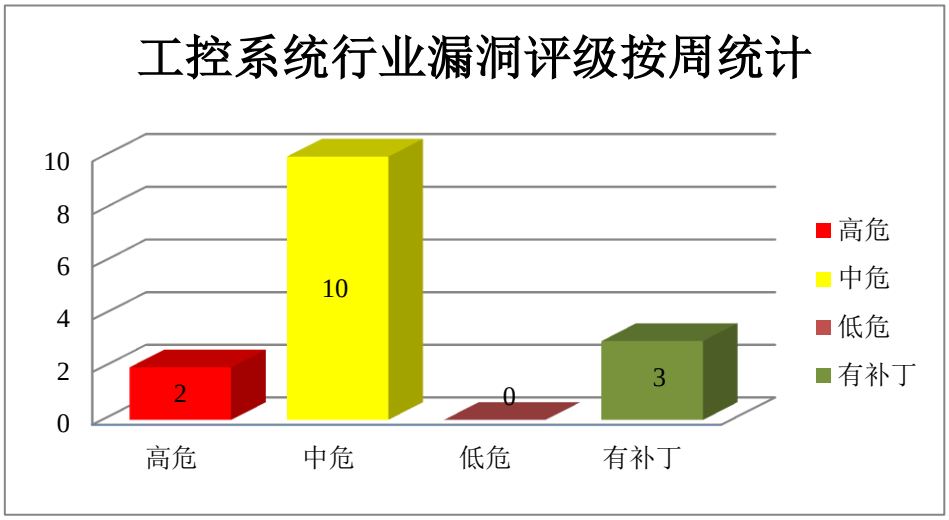

图 5 工控系统行业漏洞统计

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、NETGEAR 产品安全漏洞

NETGEAR WNR3500L 等都是美国网件（NETGEAR）公司的产品。WNR3500L 是一款无线路由器。NETGEAR D6220 是一款无线调制解调器。WN2500RP 是一款无线网络信号扩展器。NETGEAR WAC505 等都是美国网件（NETGEAR）公司的一款无线接入点（AP）。NETGEAR R6700 等都是美国网件（NETGEAR）公司的一款无线路由器。NETGEAR R7800 等都是美国网件（NETGEAR）公司的一款无线路由器。NETGEAR R8000 是美国网件（NETGEAR）公司的一款无线路由器。NETGEAR JNR1010 等都是美国网件（NETGEAR）公司的一款无线路由器。NETGEAR D7000 是一款无线调制解调器。NETGEAR WNR2020 是一款无线路由器。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受影响客户端向服务器发送非预期的请求，导致缓冲区溢出或堆溢出等。

CNVD 收录的相关漏洞包括：多款 NETGEAR 产品缓冲区溢出漏洞（CNVD-2021-59154、CNVD-2021-59157、CNVD-2021-59166）、多款 NETGEAR 产品跨站请求伪造漏洞（CNVD-2021-59156、CNVD-2021-59162、CNVD-2021-59165）、NETGEAR R8000 缓冲区溢出漏洞、NETGEAR R6700v2、R6800 和 R6900v2 缓冲区溢出漏洞。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-2021-59154

https://www.cnvd.org.cn/flaw/show/CNVD-2021-59157

https://www.cnvd.org.cn/flaw/show/CNVD-2021-59156

https://www.cnvd.org.cn/flaw/show/CNVD-2021-59158

https://www.cnvd.org.cn/flaw/show/CNVD-2021-59164

https://www.cnvd.org.cn/flaw/show/CNVD-2021-59162

https://www.cnvd.org.cn/flaw/show/CNVD-2021-59166

https://www.cnvd.org.cn/flaw/show/CNVD-2021-59165

2、Oracle 产品安全漏洞

Oracle E-Business Suite 是在原来 Application（ERP）基础上的扩展，包括 ERP（企业资源计划管理）、HR（人力资源管理）、CRM（客户关系管理）等等多种管理软件的集合，是无缝集成的一个管理套件。Oracle Workflow 是其中的可帮助交付一个完整的工作流管理系统的一系列工具。Oracle Marketing 是其中的营销软件。Oracle Public Sector Financials (International)扩展了 Oracle Financials 功能，并为公共部门机构的集成财务管理解决方案提供了基础。Oracle Collaborative Planning 是一个基于 Internet 的协作解决方案，通过提供跨虚拟供应链的协作需求、供应和库存计划的高级功能来快速显著提高供应链绩效。Oracle Outside In Technology 是一套软件开发工具包 (SDK)，为开发人员提供了一个提取、规范化、清理、转换和查看 600 多种非结构化文件格式的内容的综合解决方案。Oracle Database Server 是一个对象一关系数据库管理系统，提供开放的、全面的、集成的信息管理方法。本周，上述产品被披露存在未授权访问漏洞，攻击者可利用漏洞可能导致对关键数据或所有 Oracle Web Applications Desktop Integrator 可访问数据的未授权创建、删除或修改访问，以及对关键数据的未授权访问或对所有 Oracle Web Applications Desktop Integrator 可访问数据的完全访问等。

CNVD 收录的相关漏洞包括：Oracle Outside In Technology 存在未授权访问漏洞、Oracle E-Business Suite 未授权访问漏洞（CNVD-2021-57454、CNVD-2021-57446、CNVD-2021-57443、CNVD-2021-57442、CNVD-2021-57441、CNVD-2021-57440）、Oracle Database Server 未授权访问漏洞（CNVD-2021-57455）。其中“Oracle E-Business Suite 未授权访问漏洞（CNVD-2021-57445、CNVD-2021-57444）”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-2021-57440

https://www.cnvd.org.cn/flaw/show/CNVD-2021-57439

https://www.cnvd.org.cn/flaw/show/CNVD-2021-57443

https://www.cnvd.org.cn/flaw/show/CNVD-2021-57442

https://www.cnvd.org.cn/flaw/show/CNVD-2021-57441

https://www.cnvd.org.cn/flaw/show/CNVD-2021-57446

https://www.cnvd.org.cn/flaw/show/CNVD-2021-57455

https://www.cnvd.org.cn/flaw/show/CNVD-2021-57454

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。本周，上述产品被披露存在远程代码执行漏洞，攻击者可利用漏洞实现远程代码执行。

CNVD 收录的相关漏洞包括：Microsoft Windows 和 Windows Server 远程代码执行漏洞（CNVD-2021-58239、CNVD-2021-58238、CNVD-2021-58244、CNVD-2021-58243、CNVD-2021-58242、CNVD-2021-58241、CNVD-2021-58246、CNVD-2021-58245）。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-2021-58239
https://www.cnvd.org.cn/flaw/show/CNVD-2021-58238
https://www.cnvd.org.cn/flaw/show/CNVD-2021-58244
https://www.cnvd.org.cn/flaw/show/CNVD-2021-58243
https://www.cnvd.org.cn/flaw/show/CNVD-2021-58242
https://www.cnvd.org.cn/flaw/show/CNVD-2021-58241
https://www.cnvd.org.cn/flaw/show/CNVD-2021-58246
https://www.cnvd.org.cn/flaw/show/CNVD-2021-58245

4、Foxit 产品安全漏洞

Foxit PDF Reader 是中国福昕（Foxit）公司的一款 PDF 阅读器。本周，上述产品被披露存在远程代码执行漏洞，攻击者可利用漏洞在当前进程的上下文中执行代码。

CNVD 收录的相关漏洞包括：Foxit PDF Reader 远程代码执行漏洞（CNVD-2021-59167、CNVD-2021-59171、CNVD-2021-59170、CNVD-2021-59169、CNVD-2021-59168）、Foxit PDF Reader Annotation 远程代码执行漏洞（CNVD-2021-59175、CNVD-2021-59174、CNVD-2021-59173）。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-2021-59167
https://www.cnvd.org.cn/flaw/show/CNVD-2021-59171
https://www.cnvd.org.cn/flaw/show/CNVD-2021-59170
https://www.cnvd.org.cn/flaw/show/CNVD-2021-59169
https://www.cnvd.org.cn/flaw/show/CNVD-2021-59168
https://www.cnvd.org.cn/flaw/show/CNVD-2021-59175
https://www.cnvd.org.cn/flaw/show/CNVD-2021-59174
https://www.cnvd.org.cn/flaw/show/CNVD-2021-59173

5、QSAN 多款产品访问控制错误漏洞

QSAN SANOS 等都是中国 QSAN 公司的产品。QSAN SANOS 是 SAN 存储管理操作系统。QSAN XEVO 是一款闪存数据管理系统。QSAN Storage Manager 是一个 NAS 操作系统。本周，QSAN 多款产品被披露存在访问控制错误漏洞。攻击者可利用该漏洞发现用户凭据并通过暴力破解获得访问权限。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-2021-59058

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-2021-57420	Navigate CMS sql 注入漏洞（CNVD-2021-57420）	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/NavigateCMS/Navigate-CMS/commit/ed3f70b0083f1c2af66e9d71874619824e01350e
CNVD-2021-57445	Oracle E-Business Suite 未授权访问漏洞（CNVD-2021-57445）	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.oracle.com/security-alerts/cpujul2021.html
CNVD-2021-57461	Cisco Adaptive Security Device Manager 远程代码执行漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asdm-rce-gqjShXW
CNVD-2021-57774	CASAP Automated Enrollment SQL 注入漏洞（CNVD-2021-57774）	高	厂商已提供漏洞修补方案，请关注厂商主页及时更新：https://github.com/BigTiger2020/CASAP-Automated-Enrollment-System/blob/main/README.md
CNVD-2021-57781	SourceCodester Sales and Inventory System SQL 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://github.com/BigTiger2020/CASAP-Automated-Enrollment-System/blob/main/CASAP-Automated-Enrollment-System-2.md
CNVD-2021-58249	LOGITEC CORPORATION LAN-W300N/PGRB 操作系统命令注入漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://www.elecom.co.jp/news/security/20210126-01/
CNVD-2021-	Envoy 资源管理错误漏洞（C	高	目前厂商已发布升级补丁以修复漏

58579	NVD-2021-58579）		洞，补丁获取链接：https://github.com/envoyproxy/envoy/commit/afc39bea36fd436e54262f150c009e8d72db5014
CNVD-2021-58666	Acronis True Image 访问控制错误漏洞（CNVD-2021-58666）	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://kb.cert.org/vuls/id/114757
CNVD-2021-59059	WordPress 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.wordfence.com/blog/2021/06/easily-exploitable-critical-vulnerabilities-patched-in-profilepress-plugin/
CNVD-2021-59138	Fortinet FortiSandbox 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://www.mozilla.org/zh-CN/firefox/mobile/

小结：本周，NETGEAR 产品被披露存在多个漏洞，攻击者可利用漏洞通过受影响客户端向服务器发送非预期的请求，导致缓冲区溢出或堆溢出等。此外，Oracle、Microsoft、Foxit 等多款产品被披露存在多个漏洞，攻击者可利用漏洞可能导致对关键数据或所有 Oracle Web Applications Desktop Integrator 可访问数据的未授权创建、删除或修改访问，以及对关键数据的未授权访问或对所有 Oracle Web Applications Desktop Integrator 可访问数据的完全访问，实现远程代码执行。另外，QSAN 多款产品被披露存在访问控制错误漏洞。攻击者可利用该漏洞发现用户凭据并通过暴力破解获得访问权限。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、 MetInfo SQL 注入漏洞（CNVD-2021-59068）

验证描述

MetInfo 是中国米拓（Metinfo）公司的一套使用 PHP 和 Mysql 开发的内容管理系统（CMS）。

Metinfo 7.0 存在 SQL 注入漏洞，攻击者可利用该漏洞访问数据库敏感信息。

验证信息

POC 链接：https://github.com/Q1ngShan/PHP_Learning/issues/3

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2021-59068

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. 思科修复了 VPN 路由器中关键的高危预授权漏洞

思科已经解决了影响多个小型企业 VPN 路由器的预授权漏洞，该漏洞允许远程攻击者在易受攻击的设备上触发拒绝服务条件或执行命令和任意代码。

参考链接：https://www.bleepingcomputer.com/news/security/cisco-fixes-critical-high-severity-pre-auth-flaws-in-vpn-routers/?__cf_chl_jschl_tk__=pmd_7f32b3b28328ed018d2fdb2757c836c2a4460202-1628400973-0-gqNtZGzNAjijcnBszQvi

2. 配置错误的 Apache Hadoop YARN 正被用于挖矿

最近的一项分析揭露了网络犯罪分子是如何利用配置错误的 Apache Hadoop YARN 的。它是一种集群管理技术，也是用于执行任务的 Hadoop 框架的一部分。该报告包括有关有效载荷交付、攻击策略和基本安全建议的细节。

参考链接：https://cyware.com/news/misconfigured-apache-hadoop-yarn-exploited-for-cryptomining-abdbd6b5

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