国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2021 年 05 月 10 日-2021 年 05 月 16 日　　2021 年第 19 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 491 个，其中高危漏洞 130 个、中危漏洞 316 个、低危漏洞 45 个。漏洞平均分值为 5.77。本周收录的漏洞中，涉及 0day 漏洞 255 个（占 52%），其中互联网上出现“Dhcms 跨站脚本漏洞（CNVD-2021-34491）、NoneCMS 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 2544 个，与上周合刊（5288 个）环比减少 52%。

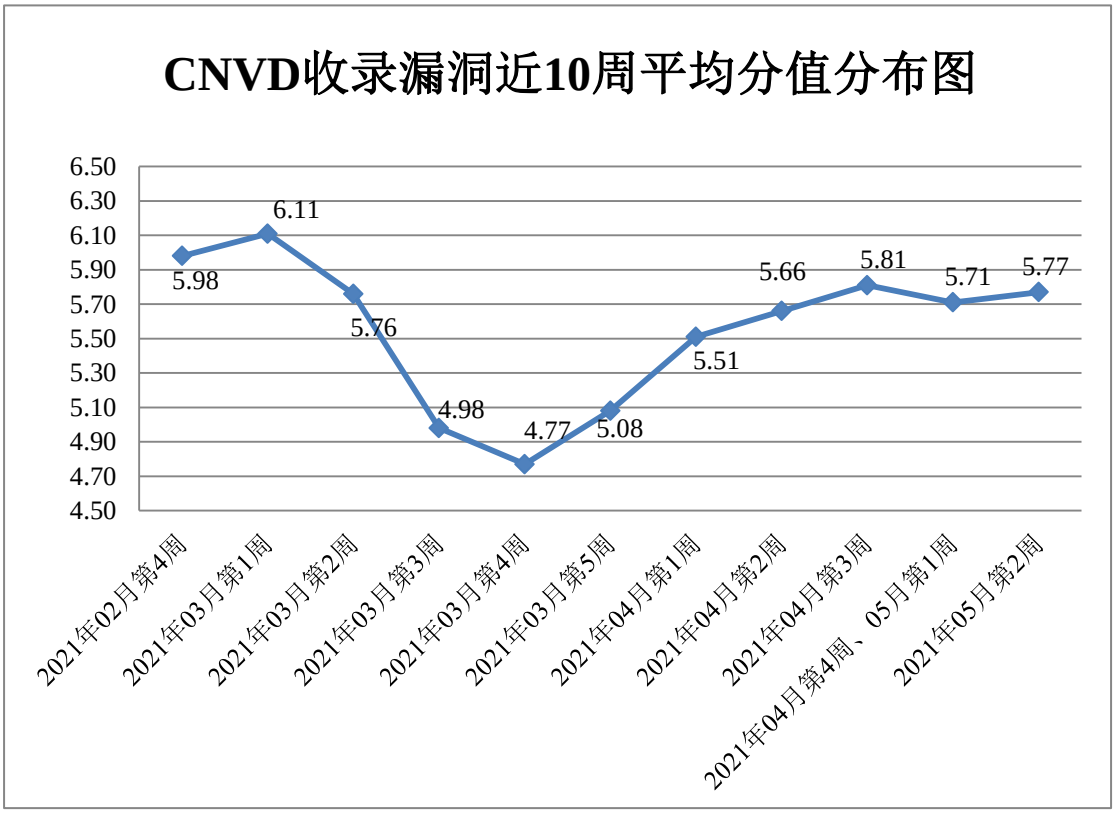

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 10 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 199 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 44 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 26 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、珠海金山办公软件有限公司、重庆远秋科技有限公司、众勤通信设备贸易（上海）有限公司、中兴通讯股份有限公司、中国电信集团有限公司、正方软件股份有限公司、浙江大华技术股份有限公司、元伸科技（股）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、用友网络科技股份有限公司、庸博（厦门）电气技术有限公司、亚美亚（中国）通讯设备有限公司、讯舟科技股份有限公司、星际（杭州）网络技术有限公司、夏普商贸（中国）有限公司、西门子（中国）有限公司、西安紫云羚网络科技有限责任公司、武汉天地伟业科技有限公司、武汉舜通智能科技有限公司、网经科技（苏州）有限公司、统信软件技术有限公司、天信仪表集团有限公司、天闻数媒科技（北京）有限公司、天津市企商汇创科技有限公司、天地伟业技术有限公司、太原易思软件技术有限公司、索尼（中国）有限公司、苏州烟火网络科技有限公司、苏州开心盒子软件有限公司、松下电器（中国）有限公司、四平市九州易通科技有限公司、施耐德电气（中国）有限公司、深圳坐标软件集团有限公司、深圳英飞拓科技股份有限公司、深圳银澎云计算有限公司、深圳市优特普技术有限公司、深圳市迅捷通信技术有限公司、深圳市网域科技技术有限公司、深圳市蓝凌软件股份有限公司、深圳市锟铻科技有限公司、深圳市吉祥腾达科技有限公司、深圳市惠尔顿信息技术有限公司、深圳市华磊信息科技有限公司、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、深圳市迪元素科技有限公司、深圳市爱思软件技术有限公司、深圳市爱德曼思科技有限公司、深圳极速创想科技有限公司、深圳和为顺网络科技有限公司、上海西默通信技术有限公司、上海七慧网络科技有限公司、上海金泓格国际贸易有限公司、上海建文软件科技有限公司、上海泛微网络科技股份有限公司、上海安硕信息技术股份有限公司、山东潍微科技股份有限公司、厦门四信通信科技有限公司、厦门狮子鱼网络科技有限公司、锐捷网络股份有限公司、青岛海威茨仪表有限公司、青岛辅德网络技术有限公司、普联技术有限公司、南京尚运网络技术有限公司、南京浩冠科技有限公司、南京冠邦网络技术有限责任公司、南昌腾速科技有限公司、南昌轨道交通集团有限公司、魅思网络科技有限公司、迈普通信技术股份有限公司、零视技术（上海）有限公司、联创互联（北京）科技有限公司、浪潮集团有限公司、廊坊市极致网络科技有

限公司、莱克斯科技(北京)有限公司、康普科技（苏州）有限公司、飓风（深圳）软件有限公司、金砖通讯科技股份有限公司、江西铭软科技有限公司、江苏沃叶软件有限公司、惠普贸易（上海）有限公司、华硕电脑（上海）有限公司、湖南奥科网络技术股份有限公司、黑龙江立高科技股份有限公司、杭州一朵云科技有限公司、杭州三一谦成科技有限公司、杭州海康威视数字技术股份有限公司、海信营销管理有限公司、海南赞赞网络科技有限公司、哈尔滨新中新电子股份有限公司、哈尔滨伟成科技有限公司、桂林天生智创信息技术有限公司、广州中思软件有限公司、广州图创计算机软件开发有限公司、广州市保伦电子有限公司、广州南方测绘科技股份有限公司、广州好智信息技术有限公司、广东盈世计算机科技有限公司、阜新教之初科技发展有限公司、福建博思软件股份有限公司、东莞市同享软件科技有限公司、东莞市冬惊鱼网络科技有限公司、成都星锐蓝海网络科技有限公司、成都万江港利科技有限公司、成都生动网络科技有限公司、成都佳发安泰教育科技股份有限公司、畅捷通信息技术股份有限公司、常州永佳软件技术有限公司、贝尔金贸易(上海)有限公司、贝尔金公司、北京中科联诚软件股份有限公司、北京亿中邮信息技术有限公司、北京星网锐捷网络技术有限公司、北京网御星云信息技术有限公司、北京硕人时代科技股份有限公司、北京软虹科技有限公司、北京派网软件有限公司、北京旷视科技有限公司、北京捷思锐科技股份有限公司、北京椒图科技有限公司、北京弘文恒瑞文化传播有限公司、北京创讯未来软件技术有限公司、北京超越无限信息技术有限公司、北京碧海威科技有限公司、北京安天网络安全技术有限公司、北京安控科技有限公司、安美世纪（北京）科技有限公司、安徽省科迅教育装备有限公司、安徽晶奇网络科技股份有限公司、《中国学术期刊（光盘版）》电子杂志社有限公司、台达集团、若依、睿谷信息、南充春杰工作室、帝国软件、WMCMS 团队、河北欧润天腾云梦吧网络工作室、WinMount、VoIPmonitor、TRENDnet、SRWare、Rockwell Automation, Inc.、Netis Systems、NETGEAR、Multilaser、Joomla!、jfinal cms、flvmeta、EZB Systems、EnGenius、EmpireCMS、Electro Industries/GaugeTech Inc.、DiYunCMS、CatfishCMS、Axis Communications AB 和 Avaya。

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，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、新华三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、北京华云安信息技术有限公司、河南灵创电子科技有限公司、北京天地和兴科技有限公司、中国电信股份有限公司网络安全产品运营中心、河南信安世纪科技有限公司、北京安帝科技有限公司、南京众智维信息科技有限公司、杭州木链物联网科技有限公司、北京远禾科技有限公司、北京墨云科技有限公司、江西省掌控者信息安全技术有限公司、星云博创科技有限公司、

山东云天安全技术有限公司、成都思维世纪科技有限公司、武汉明嘉信信息安全检测评估有限公司、北京山石网科信息技术有限公司、北京君云天下科技有限公司、小安（北京）科技有限公司、深圳市和为顺网络技术有限公司、博智安全科技股份有限公司、安徽长泰信息安全服务有限公司、北京机沃科技有限公司、深圳市魔方安全科技有限公司、上海上讯信息技术股份有限公司、上海心河信息技术有限公司、上海市信息安全测评认证中心、清远职业技术学院及其他个人白帽子向 CNVD 提交了 2544 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 1329 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）	831	831
奇安信网神（补天平台）	498	498
哈尔滨安天科技集团股份有限公司	339	0
北京神州绿盟科技有限公司	268	9
华为技术有限公司	183	0
深信服科技股份有限公司	151	0
新华三技术有限公司	128	0
北京数字观星科技有限公司	118	0
北京天融信网络安全技术有限公司	98	2
恒安嘉新（北京）科技股份公司	85	0
卫士通信息产业股份有限公司	69	0
国瑞数码零点实验室	58	0
远江盛邦（北京）网络安全科技股份有限公司	48	48
北京奇虎科技有限公司	19	19
北京启明星辰信息安全技术有限公司	2	2
南京联成科技发展股份有限公司	1	1
北京信联科汇科技有	77	77

限公司		
北京华云安信息技术有限公司	54	54
河南灵创电子科技有限公司	30	30
北京天地和兴科技有限公司	26	26
中国电信股份有限公司网络安全产品运营中心	14	14
杭州迪普科技股份有限公司	14	0
河南信安世纪科技有限公司	12	12
北京安帝科技有限公司	12	12
南京众智维信息科技有限公司	10	10
杭州木链物联网科技有限公司	9	9
北京远禾科技有限公司	7	7
北京墨云科技有限公司	6	6
江西省掌控者信息安全技术有限公司	5	5
星云博创科技有限公司	5	5
山东云天安全技术有限公司	5	5
成都思维世纪科技有限公司	5	5
武汉明嘉信信息安全检测评估有限公司	4	4
北京山石网科信息技术有限公司	4	4
北京君云天下科技有限公司	4	4
小安（北京）科技有限公司	2	2
深圳市和为顺网络技术有限公司	2	2

博智安全科技股份有限公司	2	2
安徽长泰信息安全服务有限公司	2	2
北京机沃科技有限公司	2	2
深圳市魔方安全科技有限公司	1	1
上海上讯信息技术股份有限公司	1	1
上海心河信息技术有限公司	1	1
上海市信息安全测评认证中心	1	1
清远职业技术学院	1	1
CNCERT 宁夏分中心	4	4
CNCERT 西藏分中心	1	1
个人	825	825
报送总计	4044	2544

本周漏洞按类型和厂商统计

本周，CNVD 收录了 491 个漏洞。WEB 应用 162 个，应用程序 158 个，网络设备（交换机、路由器等网络端设备）95 个，操作系统 41 个，安全产品 25 个，智能设备（物联网终端设备）5 个，数据库 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
WEB 应用	162
应用程序	158
网络设备（交换机、路由器等网络端设备）	95
操作系统	41
安全产品	25
智能设备（物联网终端设备）漏洞	5
数据库	5

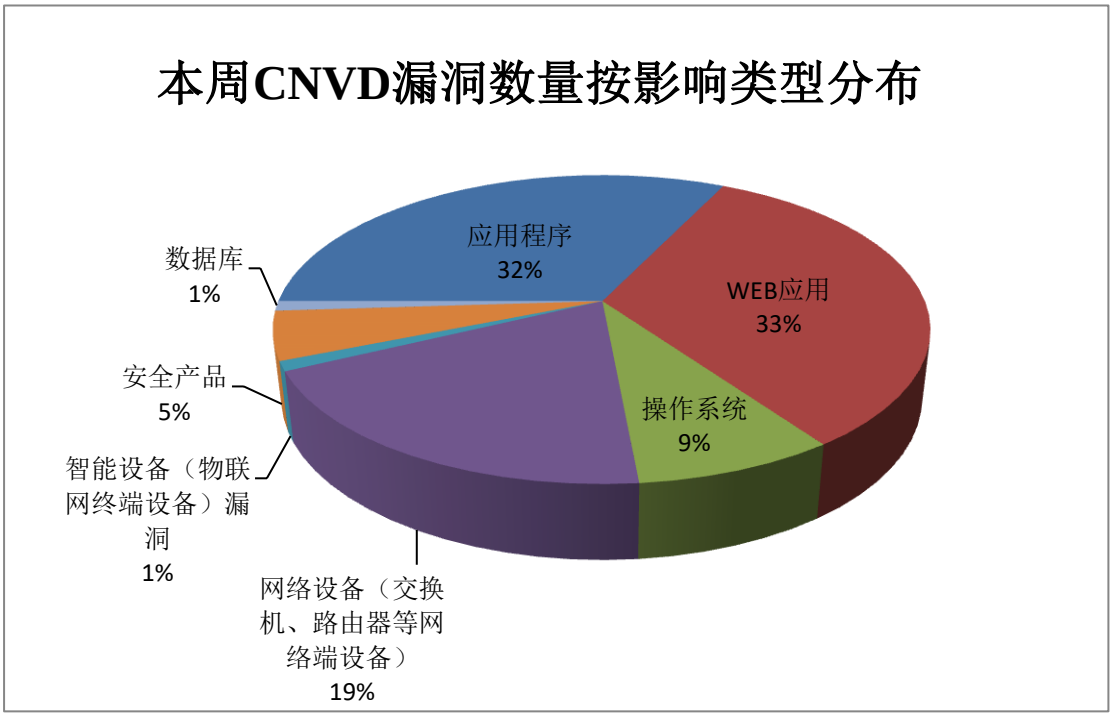

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 TP-LINK、Google、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	TP-LINK	32	7%
2	Google	29	6%
3	Oracle	28	6%
4	Parallels	21	4%
5	Microsoft	21	4%
6	Exim	15	3%
7	熊海 CMS	14	3%
8	贝尔金公司	14	3%
9	Aruba Networks	10	2%
10	其他	307	62%

本周行业漏洞收录情况

本周，CNVD 收录了 85 个电信行业漏洞，10 个移动互联网行业漏洞，8 个工控行业漏洞（如下图所示）。其中，“WAGO 跨站脚本漏洞、Delta Industrial Automation CO MMGR 远程代码执行漏洞、SIEMENS DIGSI 4 权限许可和访问控制问题漏洞、Rockwell Automation MicroLogix 1400 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/

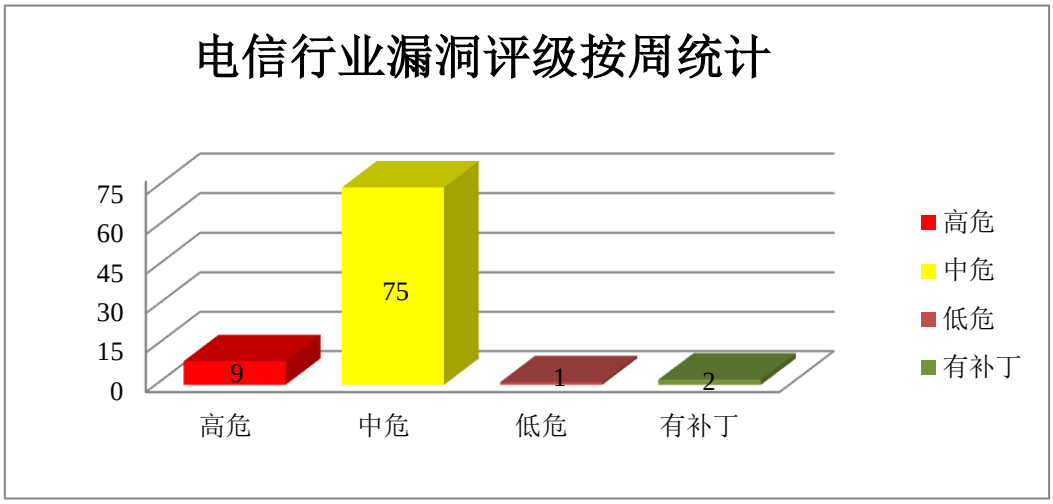

图 3 电信行业漏洞统计

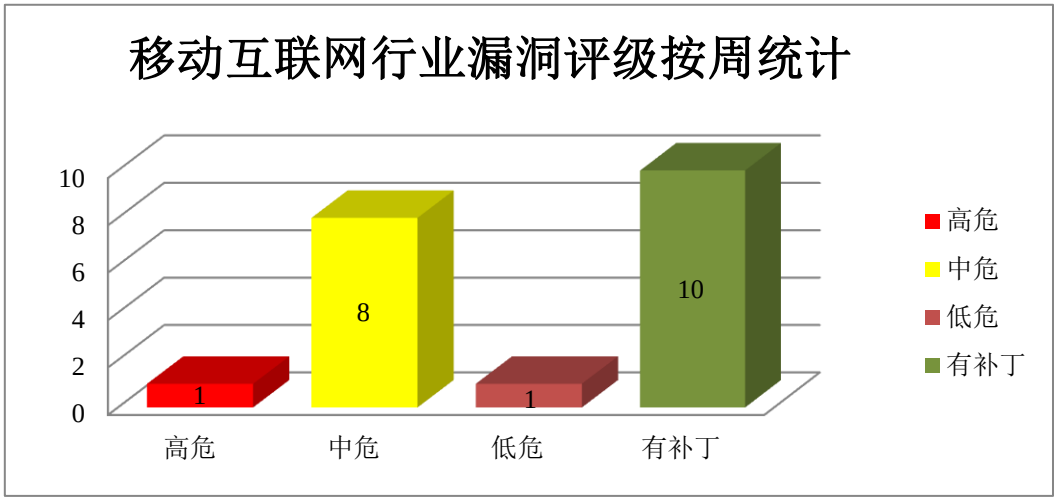

图 4 移动互联网行业漏洞统计

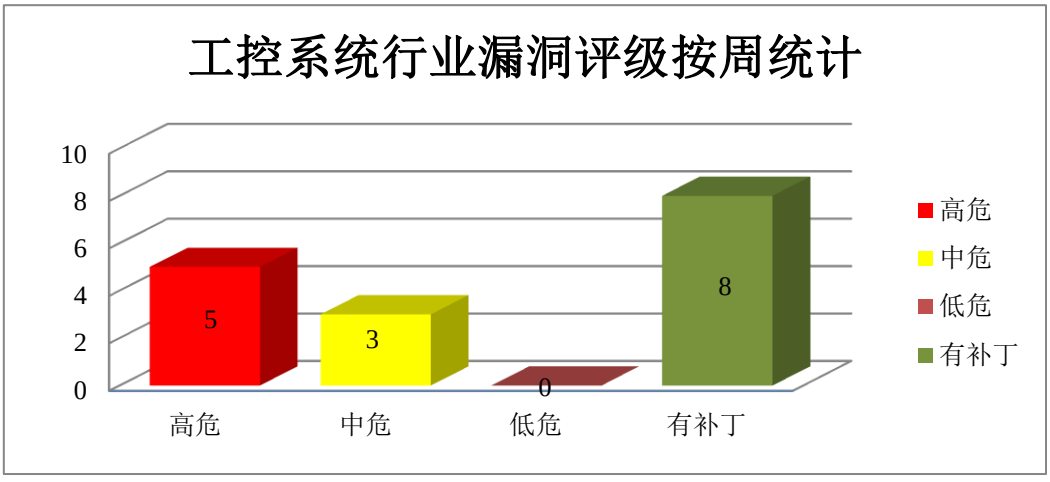

图 5 工控系统行业漏洞统计

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、Aruba Networks 产品安全漏洞

Aruba ClearPass Policy Manager 是一个应用系统提供无线网络安全接入管理系统。Aruba Networks AirWave Management Platform 是一套适用于多供应商管理的网络管理软件。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞获取敏感信息，执行任意命令，导致拒绝服务等。

CNVD 收录的相关漏洞包括：Aruba ClearPass Policy Manager 信息泄露漏洞（CNVD-2021-33523、CNVD-2021-33524）、Aruba ClearPass Policy Manager 操作系统命令注入漏洞、Aruba Networks AirWave Management Platform 命令注入漏洞（CNVD-2021-33526）、Aruba Networks AirWave Management Platform SQL 注入漏洞（CNVD-2021-33530）、Aruba Networks AirWave Management Platform XML 外部实体注入漏洞（CNVD-2021-33527、CNVD-2021-33531）、Aruba Networks AirWave Management Platform 反序列化漏洞。其中，“Aruba ClearPass Policy Manager 操作系统命令注入漏洞、Aruba Networks AirWave Management Platform 反序列化漏洞”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-2021-33523
https://www.cnvd.org.cn/flaw/show/CNVD-2021-33526
https://www.cnvd.org.cn/flaw/show/CNVD-2021-33524
https://www.cnvd.org.cn/flaw/show/CNVD-2021-33525
https://www.cnvd.org.cn/flaw/show/CNVD-2021-33530
https://www.cnvd.org.cn/flaw/show/CNVD-2021-33527
https://www.cnvd.org.cn/flaw/show/CNVD-2021-33532
https://www.cnvd.org.cn/flaw/show/CNVD-2021-33531

2、Oracle 产品安全漏洞

Oracle Secure Global Desktop 是用于运行在 Microsoft Windows、Linux、Oracle Solaris 和大型机服务器上的任何云托管企业应用程序和托管桌面的安全的远程访问解决方案。Oracle HTTP Server 是 Oracle Fusion Middleware 的 Web 服务器组件。Oracle Fusion Middleware（Oracle 融合中间件）是一套面向企业和云环境的业务创新平台。该平台提供了中间件、软件集合等功能。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多个漏洞，攻击者可利用漏洞未授权访问数据，获取敏感信息，执行任意代码等。

CNVD 收录的相关漏洞包括：Oracle Secure Global Desktop 输入验证错误漏洞（CNVD-2021-33836、CNVD-2021-33837、CNVD-2021-33838）、Oracle Fusion Middleware 输入验证错误漏洞（CNVD-2021-33844、CNVD-2021-33848）、Oracle Database Server 输入验证错误漏洞（CNVD-2021-33859、CNVD-2021-33858、CNVD-2021-33860）。其中“Oracle Secure Global Desktop 输入验证错误漏洞（CNVD-2021-33838、CNVD-2021-33837）、Oracle Fusion Middleware 输入验证错误漏洞（CNVD-2021-33848）”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-2021-33837

https://www.cnvd.org.cn/flaw/show/CNVD-2021-33836

https://www.cnvd.org.cn/flaw/show/CNVD-2021-33838

https://www.cnvd.org.cn/flaw/show/CNVD-2021-33844

https://www.cnvd.org.cn/flaw/show/CNVD-2021-33848

https://www.cnvd.org.cn/flaw/show/CNVD-2021-33859

https://www.cnvd.org.cn/flaw/show/CNVD-2021-33858

https://www.cnvd.org.cn/flaw/show/CNVD-2021-33860

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多个漏洞，攻击者可利用漏洞提升权限，远程代码执行。

CNVD 收录的相关漏洞包括：Microsoft Windows 和 Windows Server 权限提升漏洞（CNVD-2021-34474、CNVD-2021-34473、CNVD-2021-34472、CNVD-2021-34480、CNVD-2021-34479、CNVD-2021-34482、CNVD-2021-34485）、Microsoft Windows 和 Windows Server 远程代码执行漏洞（CNVD-2021-34477）。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-2021-34474

https://www.cnvd.org.cn/flaw/show/CNVD-2021-34473

https://www.cnvd.org.cn/flaw/show/CNVD-2021-34472

https://www.cnvd.org.cn/flaw/show/CNVD-2021-34477

https://www.cnvd.org.cn/flaw/show/CNVD-2021-34480

https://www.cnvd.org.cn/flaw/show/CNVD-2021-34479

https://www.cnvd.org.cn/flaw/show/CNVD-2021-34482

https://www.cnvd.org.cn/flaw/show/CNVD-2021-34485

4、Google 产品安全漏洞

Google Chrome 是美国谷歌（Google）公司的一款 Web 浏览器。Google Android 是一套以 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，攻击者可利用漏洞绕过安全限制，提升权限。

CNVD 收录的相关漏洞包括：Google Chrome V8 安全绕过漏洞、Google Android 竞争条件问题漏洞、Google Android 权限提升漏洞（CNVD-2021-34547、CNVD-2021-34546、CNVD-2021-34550、CNVD-2021-34549、CNVD-2021-34548）、Google Android 存在权限提升漏洞（CNVD-2021-34551）。其中，“Google Chrome V8 安全绕过漏洞”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-2021-34523
https://www.cnvd.org.cn/flaw/show/CNVD-2021-34547
https://www.cnvd.org.cn/flaw/show/CNVD-2021-34546
https://www.cnvd.org.cn/flaw/show/CNVD-2021-34545
https://www.cnvd.org.cn/flaw/show/CNVD-2021-34550
https://www.cnvd.org.cn/flaw/show/CNVD-2021-34549
https://www.cnvd.org.cn/flaw/show/CNVD-2021-34548
https://www.cnvd.org.cn/flaw/show/CNVD-2021-34551

5、OpenClinic GA SQL 注入漏洞（CNVD-2021-34496）

OpenClinic GA 是一款开源医院综合信息管理系统。本周，OpenClinic GA 被披露存在 SQL 注入漏洞。攻击者可通过特制 HTTP 请求利用该漏洞进行 SQL 注入攻击。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-2021-34496

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-2021-33863	Netop Vision Pro 访问控制错误漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.netop.com/
CNVD-2021-33866	SIEMENS DIGSI 4 权限许可和访问控制问题漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://cert-portal.siemens.com/productcert/pdf/ssa-536315.pdf
CNVD-2021-34186	Parallels Desktop OTG 堆缓冲区溢出漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://kb.parallels.com/en/125013

CNVD-2021-34258	e-office 泛微协同办公系统存在文件上传漏洞	高	厂商已提供漏洞修补方案，建议用户下载使用：http://v10.e-office.cn/9safepack/泛微 e-office9.5 20210427 补丁程序.zip
CNVD-2021-34350	Trend Micro Home Network Security 拒绝服务漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://helpcenter.trendmicro.com/en-us/article/TMKA-10312
CNVD-2021-34535	Exim 释放后重用漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.exim.org/
CNVD-2021-34731	ZZCMS 密码重置漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：http://www.zzcms.net/about/6.htm
CNVD-2021-34728	WAGO 跨站脚本漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://wago.io/
CNVD-2021-34732	Adobe After Effects 越界写入漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://helpx.adobe.com/security/products/after_effects/apsb21-33.html
CNVD-2021-34749	Foxit Reader 代码执行漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.foxitsoftware.com/support/security-bulletins.html

小结：本周，Aruba Networks 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，执行任意命令，导致拒绝服务等。此外，Oracle、Microsoft、Google 等多款产品被披露存在多个漏洞，攻击者可利用漏洞绕过安全限制，提升权限，执行任意代码等。另外，OpenClinic GA 被披露存在 SQL 注入漏洞。攻击者可通过特制 HTTP 请求利用该漏洞进行 SQL 注入攻击。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、NoneCMS 跨站脚本漏洞

验证描述

NoneCMS 是一款简单小巧的开源内容管理系统，可快速搭建企业站、个人博客，并且支持移动端。

NoneCMS 1.3.0 版本中的 admin/article/add.html 存在跨站脚本漏洞。攻击者可通过

name 参数利用该漏洞注入任意 Web 脚本或 HTML。

验证信息

POC 链接：https://github.com/nangge/noneCms/issues/32

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2021-34499

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. 披露后六个月，思科在 VPN 产品中修补了代码执行漏洞

该漏洞最初于 2020 年 11 月披露，该漏洞影响安全 VPN 应用程序的进程间通信（IPC）通道，并且可能被本地攻击者滥用以导致 AnyConnect 用户运行恶意脚本。

参考链接：https://www.securityweek.com/cisco-patches-code-execution-flaw-vpn-product-6-months-after-disclosure

2. 所有 Wi-Fi 设备皆存在 FragAttacks 漏洞，个人信息可能因此遭窃

知名网络安全研究人员 Mathy Vanhoef 发表一系列 Wi-Fi 设备安全漏洞，这些漏洞被统称为 FragAttacks，是碎片（Fragmentation）以及聚合攻击（Aggregation Attacks）的组合字，全球 Wi-Fi 设备无一幸免，连最新的 WPA3 规范都存在设计缺陷。位在受害者无线电范围内的攻击者，可以利用 FragAttacks 漏洞窃取用户信息并且攻击设备。

参考链接：https://www.cnbeta.com/articles/tech/1127089.htm

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