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 23 日-2021 年 08 月 29 日 **2021 年第 34 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 485 个，其中高危漏洞 127 个、中危漏洞 319 个、低危漏洞 39 个。漏洞平均分值为 5.69。本周收录的漏洞中，涉及 0day 漏洞 272 个（占 56%），其中互联网上出现“Wuzhi CMS SQL 注入漏洞（CNVD-2021-66056）、Nuance Winscribe Dictation SQL 注入漏洞”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原创漏洞总数 15481 个，与上周（12901 个）环比增加 20%。

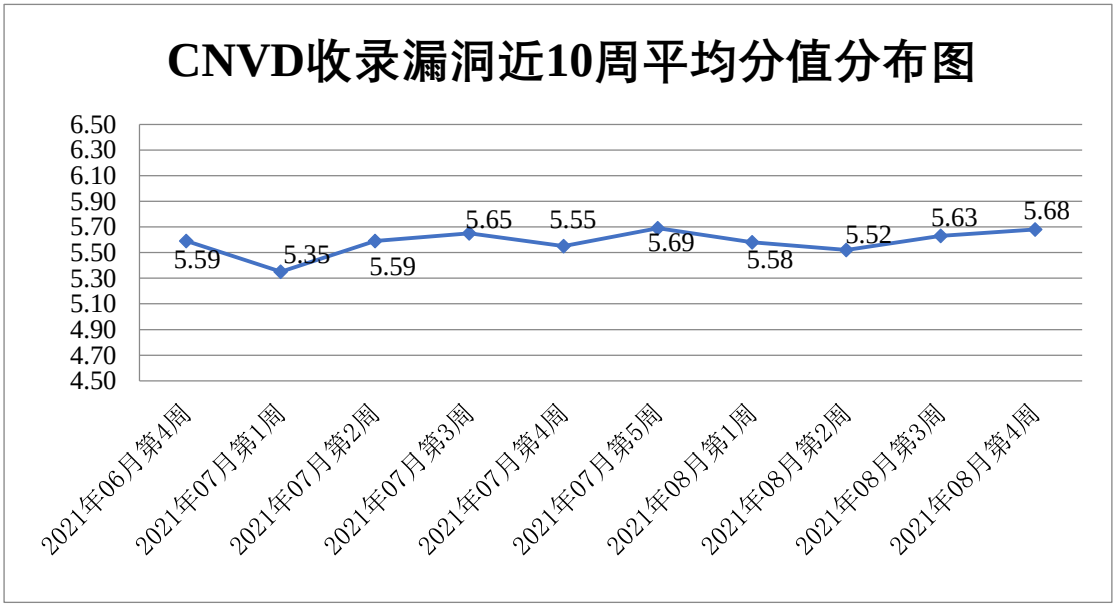

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 21 起，向基础电信企业通报漏洞事件 49 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 756 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 46 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 64 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、珠海高凌信息科技股份有限公司、重庆市武隆喀斯特旅游产业（集团）有限公司、郑州晨华科技有限公司、正方软件股份有限公司、浙江大华技术股份有限公司、友讯电子设备（上海）有限公司、新天科技股份有限公司、欣然影视文化艺术有限公司、西安启莱软件科技有限公司、西安福禄传承网络科技有限公司、武汉天地伟业科技有限公司、微软（中国）有限公司、网件（北京）网络技术有限公司、天津天堰科技股份有限公司、特斯拉（上海）有限公司、苏州梦图地理信息系统有限责任公司、苏州科达科技股份有限公司、四川迅睿云软件开发有限公司、思科系统（中国）网络技术有限公司、曙光信息产业股份有限公司、世邦通信股份有限公司、石家庄市征红网络科技有限公司、石家庄和嘉科技有限公司、深圳维盟科技股份有限公司、深圳市中电电力技术股份有限公司、深圳市万网博通科技有限公司、深圳市同为数码科技股份有限公司、深圳市企慧通信息技术有限公司、深圳市美科星通信技术有限公司、深圳市吉祥腾达科技有限公司、深圳市鼎游信息技术有限公司、深圳市必联电子有限公司、深圳齐心好视通云计算有限公司、深圳警翼智能科技股份有限公司、深圳华磊物流通信息科技有限公司、上海羿石软件科技有限公司、上海瑞策软件有限公司、上海纽盾科技股份有限公司、上海穆云智能科技有限公司、上海莱澳信息科技有限公司、上海华测导航技术股份有限公司、上海覆盆子信息科技有限公司、上海复兆信息技术有限公司、上海泛微网络科技股份有限公司、山东云时空信息科技有限公司、山东潍微科技股份有限公司、山东康程信息科技有限公司、山东开创云计算有限公司、厦门四信通信科技有限公司、厦门得推网络科技有限公司、三星（中国）投资有限公司、润申信息科技（上海）有限公司、瑞斯康达科技发展股份有限公司、日冲商业（北京）有限公司、青岛灼灼文化传媒有限公司、普联技术有限公司、南宁市青秀区经济贸易和信息化局、南京通达海科技股份有限公司、南京墨博云舟信息科技有限公司、南京科远智慧科技集团股份有限公司、魔秀科技（北京）股份有限公司、聯盟電子科技股份有限公司、朗坤智慧科技股份有限公司、金华市宁志网络科技有限公司、江西铭软科技有限公司、江西金磊科技发展有限公司、江苏卓易信息科技股份有限公司、江苏银行股份有限公司、惠普贸易（上海）有限公司、华硕电脑（上海）有限公司、虎扑（上海）文化传播股份有限公司、湖南壹拾捌号网络技术有限公司、湖南天烽科技有限公司、湖南建研信息技术股份有限公司、洪湖尔创网联信息技术有限公司、杭州中宝科技有限公司、杭州先锋电子技术股份有限公司、海南赞赞网络科技有限公司、哈尔滨会图科技有限公司、广州向日葵保险经纪有限公司、广州图创计算机软件开发有限公司、广州京

思顿电子科技有限公司、广州安网通信技术有限公司、抚顺英特网络科技开发有限公司、福建四创软件有限公司、佛山市杜特软件科技有限公司、飞利浦（中国）投资有限公司、东营金石软件有限公司、东华软件股份公司、大庆紫金桥软件技术有限公司、橙树网络技术有限公司、成都极米科技股份有限公司、沧州市凡诺广告传媒有限公司、北京中广上洋科技股份有限公司、北京致远互联软件股份有限公司、北京因酷时代科技有限公司、北京星网锐捷网络技术有限公司、北京小米科技有限责任公司、北京微鲤科技有限公司、北京威速科技有限公司、北京网御星云信息技术有限公司、北京网测科技有限公司、北京硕人时代科技股份有限公司、北京神州数码云科信息技术有限公司、北京珑大钜商科技有限公司、北京景点通科技有限公司、北京火木科技有限公司、北京国炬信息技术有限公司、北京峰趣互联网信息服务有限公司、北京北森云计算股份有限公司、傲拓科技股份有限公司、爱普生（中国）有限公司、帝国软件、广东省农村信用社联合社、若依、狂雨小说 cms、快排 CMS、FineCMS、DM 企业建站系统、梦想 cms、鱼跃 CMS、MyfCMS-闵益飞内容管理系统、Yasm、Webod、ThinkCMF、The Apache Software Foundation、TaoCMS、SeaCMS、NETGEAR、MuYuCMS、maccms、kyan 和 Catfish CMS。

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、北京数字观星科技有限公司、北京启明星辰信息安全技术有限公司、北京奇虎科技有限公司等单位报送公开收集的漏洞数量较多。北京山石网科信息技术有限公司、中国电信股份有限公司网络安全产品运营中心、山东云天安全技术有限公司、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、河南信安世纪科技有限公司、内蒙古洞明科技有限公司、山东新潮信息技术有限公司、内蒙古云科数据服务股份有限公司、河南灵创电子科技有限公司、上海纽盾科技股份有限公司、亚信科技（成都）有限公司、南京众智维信息科技有限公司、信联科技（南京）有限公司、泰山信息科技有限公司、北京安帝科技有限公司、北京天地和兴科技有限公司、广东蓝爵网络安全技术股份有限公司、北京惠而特科技有限公司、江苏快页信息技术有限公司、重庆贝特计算机系统工程有限公司、武汉明嘉信信息安全检测评估有限公司、重庆都会信息科技有限公司、宁波和利时信息安全研究院、北京信联科汇科技有限公司、海南神州希望网路有限公司、北京云科安信科技有限公司（Seraph 安全实验室）、长春嘉诚信息技术股份有限公司、北京云弈科技有限公司、腾讯安全应急响应中心、河南天祺信息安全技术有限公司、平安银河实验室、浙江木链物联网科技有限公司、北京顶象技术有限公司、江苏保旺达软件技术有限公司、杭州美创科技有限公司、四川赛虎科技有限公司、广州安亿信软件科技有限公司、北京远禾科技有限公司、东方电气集团科学技术研究院有限公司能源装备工控网络安全工程实验室、星云博创科技有限公司、广州乐轩玄

彩电子科技有限公司、浙江国利网安科技有限公司、北京机沃科技有限公司、江苏翔信信息安全技术有限公司及其他个人白帽子向 CNVD 提交了 15481 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 12013 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
奇安信网神（补天平台）	10825	10825
斗象科技（漏洞盒子）	766	766
上海交大	422	422
北京神州绿盟科技有限公司	388	10
哈尔滨安天科技集团股份有限公司	265	0
北京数字观星科技有限公司	226	0
北京启明星辰信息安全技术有限公司	100	45
北京奇虎科技有限公司	99	41
新华三技术有限公司	99	0
华为技术有限公司	97	0
恒安嘉新（北京）科技股份公司	86	0
深信服科技股份有限公司	79	1
卫士通信息产业股份有限公司	65	65
天津市国瑞数码安全系统股份有限公司	59	0
远江盛邦（北京）网络安全科技股份有限公司	45	45
北京天融信网络安全技术有限公司	11	11

南京联成科技发展股份有限公司	6	6
浙江大华技术股份有限公司	4	4
内蒙古奥创科技有限公司	2	2
北京山石网科信息技术有限公司	397	397
中国电信股份有限公司网络安全产品运营中心	376	376
北京华顺信安科技有限公司	265	0
山东云天安全技术有限公司	228	228
联想集团	197	0
北京华云安信息技术有限公司	178	178
杭州海康威视数字技术股份有限公司	122	122
河南信安世纪科技有限公司	60	60
内蒙古洞明科技有限公司	53	53
山东新潮信息技术有限公司	48	48
内蒙古云科数据服务股份有限公司	47	47
河南灵创电子科技有限公司	44	44
上海纽盾科技股份有限公司	40	40
亚信科技（成都）有限公司	33	1
南京众智维信息科技	31	31

有限公司		
信联科技（南京）有限公司	26	26
泰山信息科技有限公司	23	23
北京安帝科技有限公司	23	23
北京天地和兴科技有限公司	21	21
广东蓝爵网络安全技术股份有限公司	21	21
北京惠而特科技有限公司	19	19
杭州迪普科技股份有限公司	14	0
江苏快页信息技术有限公司	12	12
重庆贝特计算机系统工程有限公司	12	12
武汉明嘉信信息安全检测评估有限公司	10	10
重庆都会信息科技有限公司	9	9
宁波和利时信息安全研究院	9	9
北京信联科汇科技有限公司	7	7
海南神州希望网路有限公司	7	7
北京云科安信科技有限公司（Seraph 安全实验室）	6	6
长春嘉诚信息技术股份有限公司	5	5
北京云弈科技有限公	5	5

司		
腾讯安全应急响应中心	5	5
河南天祺信息安全技术有限公司	4	4
平安银河实验室	4	4
浙江木链物联网科技有限公司	4	4
北京顶象技术有限公司	3	3
江苏保旺达软件技术有限公司	3	3
杭州美创科技有限公司	3	3
四川赛虎科技有限公司	2	2
广州安亿信软件科技有限公司	2	2
北京远禾科技有限公司	2	2
东方电气集团科学技术研究院有限公司能源装备工控网络安全工程实验室	1	1
星云博创科技有限公司	1	1
广州乐轩玄彩电子科技有限公司	1	1
浙江国利网安科技有限公司	1	1
北京机沃科技有限公司	1	1
江苏翔信信息安全技术有限公司	1	1
个人	1360	1360

报送总计	17390	15481

本周漏洞按类型和厂商统计

本周，CNVD 收录了 485 个漏洞。WEB 应用 188 个，应用程序 117 个，操作系统 109 个，网络设备（交换机、路由器等网络端设备）43 个，智能设备（物联网终端设备）20 个，安全产品 7 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	188
应用程序	117
操作系统	109
网络设备（交换机、路由器等网络端设备）	43
智能设备（物联网终端设备）	20
安全产品	7
数据库	1

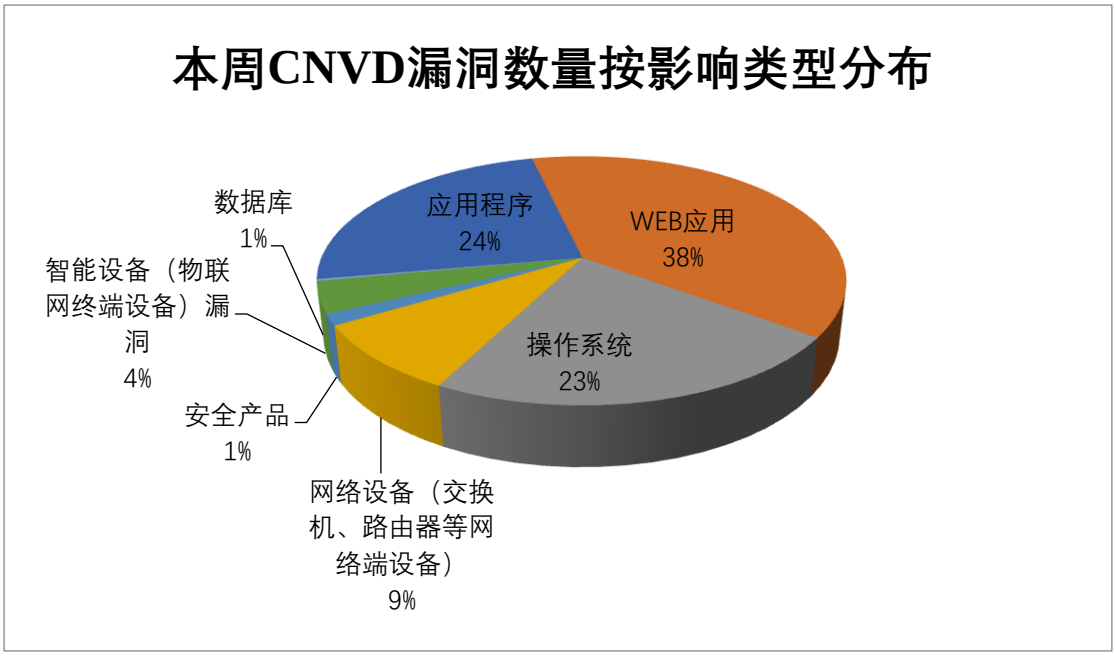

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Microsoft、Huawei、F5 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	Microsoft	72	15%

2	Huawei	41	8%
3	F5	29	6%
4	Google	26	5%
5	Foxit	13	3%
6	北京星网锐捷网络技术有限公司	13	3%
7	北京因酷时代科技有限公司	13	3%
8	智伟 CMS	12	2%
9	GPAC	10	2%
10	其他	256	53%

本周行业漏洞收录情况

本周，CNVD 收录了 25 个电信行业漏洞，66 个移动互联网行业漏洞，7 个工控行业漏洞（如下图所示）。其中，“Huawei EMUI/Magic UI 基于 NFC 连接身份验证漏洞、Huawei EMUI/Magic UI 不正确验证漏洞”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/

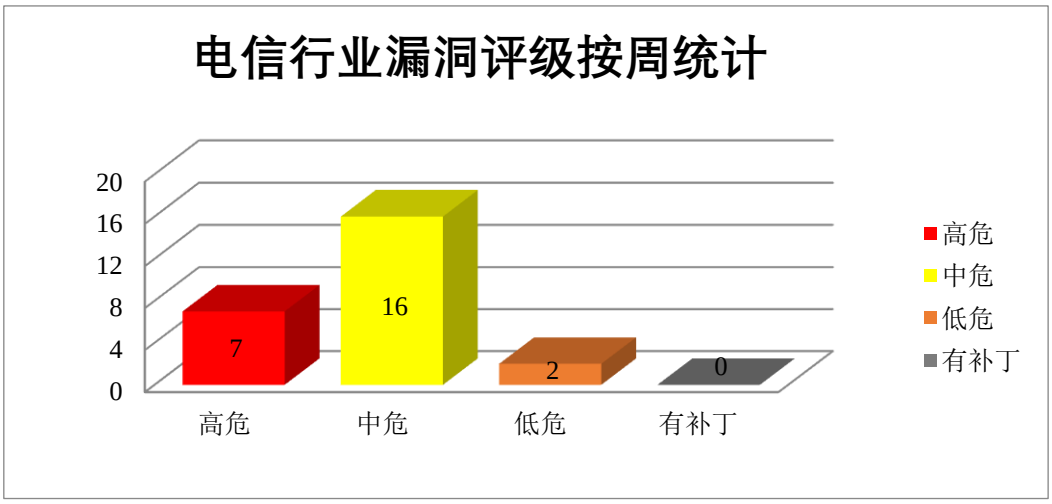

图 3 电信行业漏洞统计

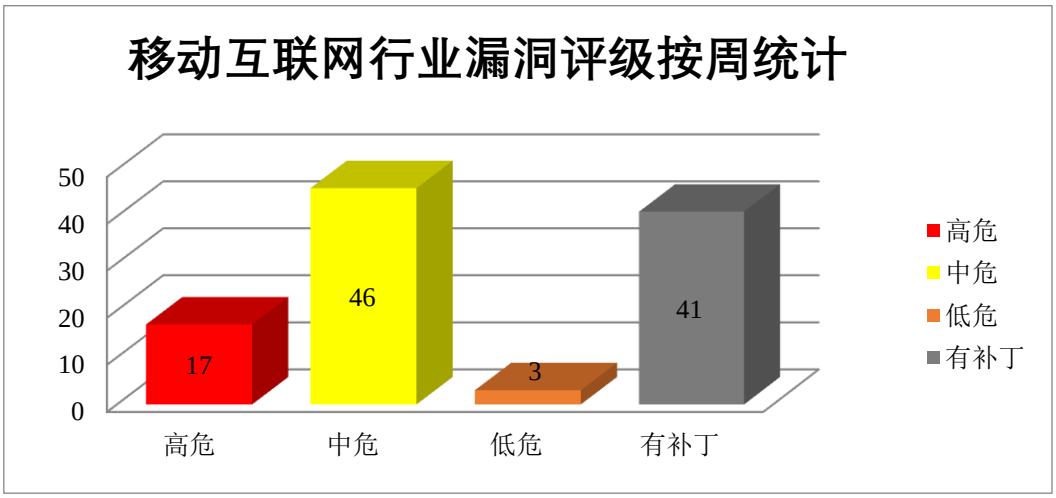

图 4 移动互联网行业漏洞统计

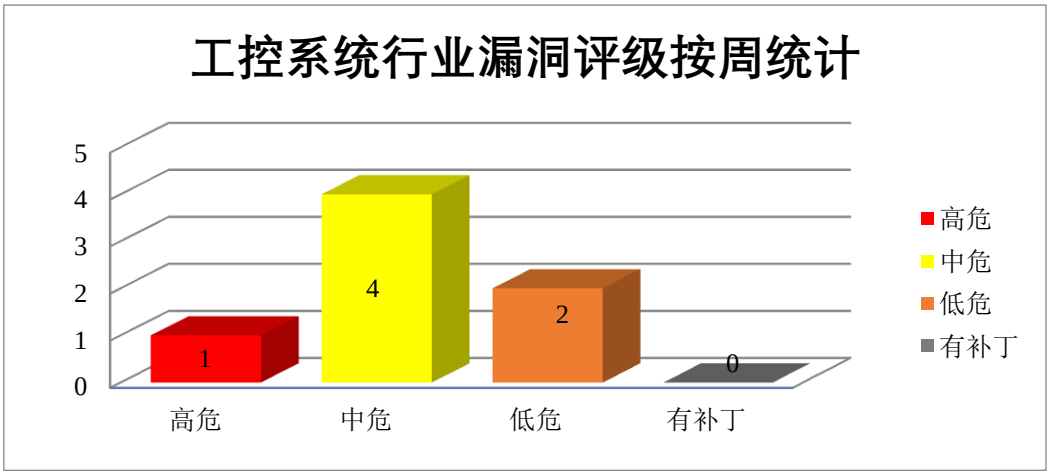

图 5 工控系统行业漏洞统计

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、F5 产品安全漏洞

F5 BIG-IP 是 F5 公司的一款集成了网络流量编排、负载均衡。智能 DNS，远程接入策略管理等功能的应用交付平台。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞在当前登录用户的上下文中执行 JavaScript，在 BIG-IP 系统上造成拒绝服务等。

CNVD 收录的相关漏洞包括：F5 BIG-IP TMUI 跨站脚本漏洞、F5 BIG-IP Advanced WAF and ASM TMUI 服务端请求伪造漏洞、F5 BIG-IP TMM 拒绝服务漏洞（CNVD-2021-65649、CNVD-2021-65648、CNVD-2021-65647）、F5 BIG-IP DNS 拒绝服务漏洞、F5 BIG-IP Advanced WAF and ASM WebSocket 拒绝服务漏洞、F5 BIG-IP TMUI 远程命令执行漏洞。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-2021-65623
https://www.cnvd.org.cn/flaw/show/CNVD-2021-65621
https://www.cnvd.org.cn/flaw/show/CNVD-2021-65649
https://www.cnvd.org.cn/flaw/show/CNVD-2021-65648
https://www.cnvd.org.cn/flaw/show/CNVD-2021-65647
https://www.cnvd.org.cn/flaw/show/CNVD-2021-65651
https://www.cnvd.org.cn/flaw/show/CNVD-2021-65650
https://www.cnvd.org.cn/flaw/show/CNVD-2021-65655

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。本周，上述产品被披露存在远程代码执行漏洞，攻击者可利用该漏洞在当前用户的上下文中执行任意代码。

CNVD 收录的相关漏洞包括：Microsoft Windows/Windows Server 远程代码执行漏洞（CNVD-2021-65596、CNVD-2021-65602、CNVD-2021-65601、CNVD-2021-65600 CNVD-2021-65599、CNVD-2021-65605、CNVD-2021-65604、CNVD-2021-65603）。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-2021-65596
https://www.cnvd.org.cn/flaw/show/CNVD-2021-65602
https://www.cnvd.org.cn/flaw/show/CNVD-2021-65601
https://www.cnvd.org.cn/flaw/show/CNVD-2021-65600
https://www.cnvd.org.cn/flaw/show/CNVD-2021-65599
https://www.cnvd.org.cn/flaw/show/CNVD-2021-65605
https://www.cnvd.org.cn/flaw/show/CNVD-2021-65604
https://www.cnvd.org.cn/flaw/show/CNVD-2021-65603

3、Foxit 产品安全漏洞

Foxit PDF Reader（旧名：Foxit Reader）是一套用来阅读 PDF 格式文件的软件，由福建福昕软件所研发。本周，上述产品被披露存在释放后重用漏洞漏洞，攻击者可利用该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 释放后重用漏洞（CNVD-2021-64088、CNVD-2021-64087、CNVD-2021-64090、CNVD-2021-64089、CNVD-2021-64092、CNVD-2021-64091、CNVD-2021-64093、CNVD-2021-64096）。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-2021-64088
https://www.cnvd.org.cn/flaw/show/CNVD-2021-64087
https://www.cnvd.org.cn/flaw/show/CNVD-2021-64090
https://www.cnvd.org.cn/flaw/show/CNVD-2021-64089
https://www.cnvd.org.cn/flaw/show/CNVD-2021-64092
https://www.cnvd.org.cn/flaw/show/CNVD-2021-64091
https://www.cnvd.org.cn/flaw/show/CNVD-2021-64093
https://www.cnvd.org.cn/flaw/show/CNVD-2021-64096

4、Huawei 产品安全漏洞

Huawei Emui 是一款基于 Android 开发的移动端操作系统。Huawei Magic UI 是荣耀手机的操作系统。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞导致代码注入，远程执行命令，获取系统权限等。

CNVD 收录的相关漏洞包括：Huawei EMUI/Magic UI 输入验证漏洞（CNVD-2021-64497、CNVD-2021-64498）、Huawei EMUI/Magic UI 内存地址越界漏洞、Huawei EMUI/Magic UI 整数溢出漏洞（CNVD-2021-64510、CNVD-2021-64524）、Huawei EMUI/Magic UI 反序列化漏洞、Huawei EMUI/Magic UI UAF 漏洞、Huawei EMUI/Magic UI 权限控制漏洞。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-2021-64497
https://www.cnvd.org.cn/flaw/show/CNVD-2021-64496
https://www.cnvd.org.cn/flaw/show/CNVD-2021-64498
https://www.cnvd.org.cn/flaw/show/CNVD-2021-64510
https://www.cnvd.org.cn/flaw/show/CNVD-2021-64509
https://www.cnvd.org.cn/flaw/show/CNVD-2021-64512
https://www.cnvd.org.cn/flaw/show/CNVD-2021-64511
https://www.cnvd.org.cn/flaw/show/CNVD-2021-64524

5、TOTOLINK A3002R 跨站脚本漏洞

TOTOLINK A3002RU 是一款 AC1200 无线双频千兆路由器。本周，TOTOLINK A3002R 被披露存在跨站脚本漏洞。攻击者可通过修改“服务名称”字段利用该漏洞执行任意 JavaScript。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-2021-64486

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-2021-64547	IBM Cloud Pak for Security 命令执行漏洞	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.ibm.com/blogs/psirt/security-bulletin-cloud-pak-for-security-has-several-security-vulnerabilities-addressed-in-the-latest-version/
CNVD-2021-65633	F5 BIG-IP Advanced WAF and ASM WebSocket 拒绝服务漏洞（CNVD-2021-65633）	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.f5.com/csp/article/K42051445
CNVD-2021-64499	Huawei EMUI/Magic UI 不正确验证漏洞（CNVD-2021-64499）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://consumer.huawei.com/en/support/bulletin/2021/6/
CNVD-2021-64083	GPAC Project on Advanced Content 整数溢出漏洞（CNVD-2021-64083）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://gpac.wp.imt.fr/
CNVD-2021-65654	F5 BIG-IP iControl SOAP CSRF 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.f5.com/csp/article/K53854428
CNVD-2021-64077	GPAC Project on Advanced Content 整数溢出漏洞（CNVD-2021-64077）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://gpac.wp.imt.fr/
CNVD-2021-64076	GPAC Project on Advanced Content 整数溢出漏洞（CNVD-2021-64076）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://gpac.wp.imt.fr/
CNVD-2021-65646	F5 BIG-IP TMUI XSS 漏洞（CNVD-2021-65646）	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.f5.com/csp/article/K21435974
CNVD-2021-66109	Microsoft Windows/Windows Server 权限提升漏洞（CNVD-2021-66109）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2020-17010
CNVD-2021-64079	GPAC Project on Advanced Content 整数溢出漏洞（CNVD-2021-64079）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://gpac.wp.imt.fr/

小结：本周，F5 产品被披露存在多个漏洞，攻击者可利用漏洞在当前登录用户的

上下文中执行 JavaScript，在 BIG-IP 系统上造成拒绝服务等。此外，Microsoft、Foxit、Huawei 等多款产品被披露存在多个漏洞，攻击者可利用该漏洞在当前用户的上下文中执行任意代码，导致代码注入，远程执行命令，获取系统权限等。另外，TOTOLINK A3002R 被披露存在跨站脚本漏洞。攻击者可通过修改“服务名称”字段利用该漏洞执行任意 JavaScript。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、Nuance Winscribe Dictation SQL 注入漏洞

验证描述

Nuance Winscribe Dictation 是 Nuance 公司的一款自动化的工作流解决方案。以更高效、更灵活的方式创建和共享高质量文档并简化复杂的工作流程。

Nuance Winscribe Dictation 4.1.0.99 存在 SQL 注入漏洞，该漏洞源于软件 Exporter 中的 exporter/Login.aspx 的登录表单未进行有效的校验，未经身份验证的远程，攻击者可利用该漏洞通过 txtPassword 参数读取数据库。

验证信息

POC 链接：https://slazarus.xyz/winscribe.html

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2021-66055

信息提供者

北京华顺信安科技有限公司

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. 微软对其云计算数据库漏洞发出警告

微软 8 月 26 日对其数以千计的云计算客户发出警告，攻击者可能允许读取、改变甚至删除他们的主数据库。这些客户中包括一些全球最大的公司。该漏洞存在于微软 Azure 的旗舰产品 Cosmos 数据库。

参考链接：https://www.solidot.org/story?sid=68708

2. Realtek 漏洞使数十个品牌面临供应链攻击

目前，中国台湾半导体公司 Realtek 芯片组中的一个漏洞 CVE-2021-35395 影响了来自 65 家供应商的 200 多种 Wi-Fi 和路由器产品。

参考链接：https://www.zdnet.com/article/realtek-hardware-bugs-expose-dozens-of-brands-to-supply-chain-cyber-attack/

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