国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2022 年 10 月 24 日-2022 年 10 月 30 日 **2022 年第 43 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 508 个，其中高危漏洞 222 个、中危漏洞 211 个、低危漏洞 75 个。漏洞平均分值为 6.08。本周收录的漏洞中，涉及 0day 漏洞 346 个（占 68%），其中互联网上出现“BloofoxCms SQL 注入漏洞、ZZCMS 跨站脚本漏洞（CNVD-2022-71404）”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漏洞总数 13636 个，与上周（25769 个）环比减少 47%。

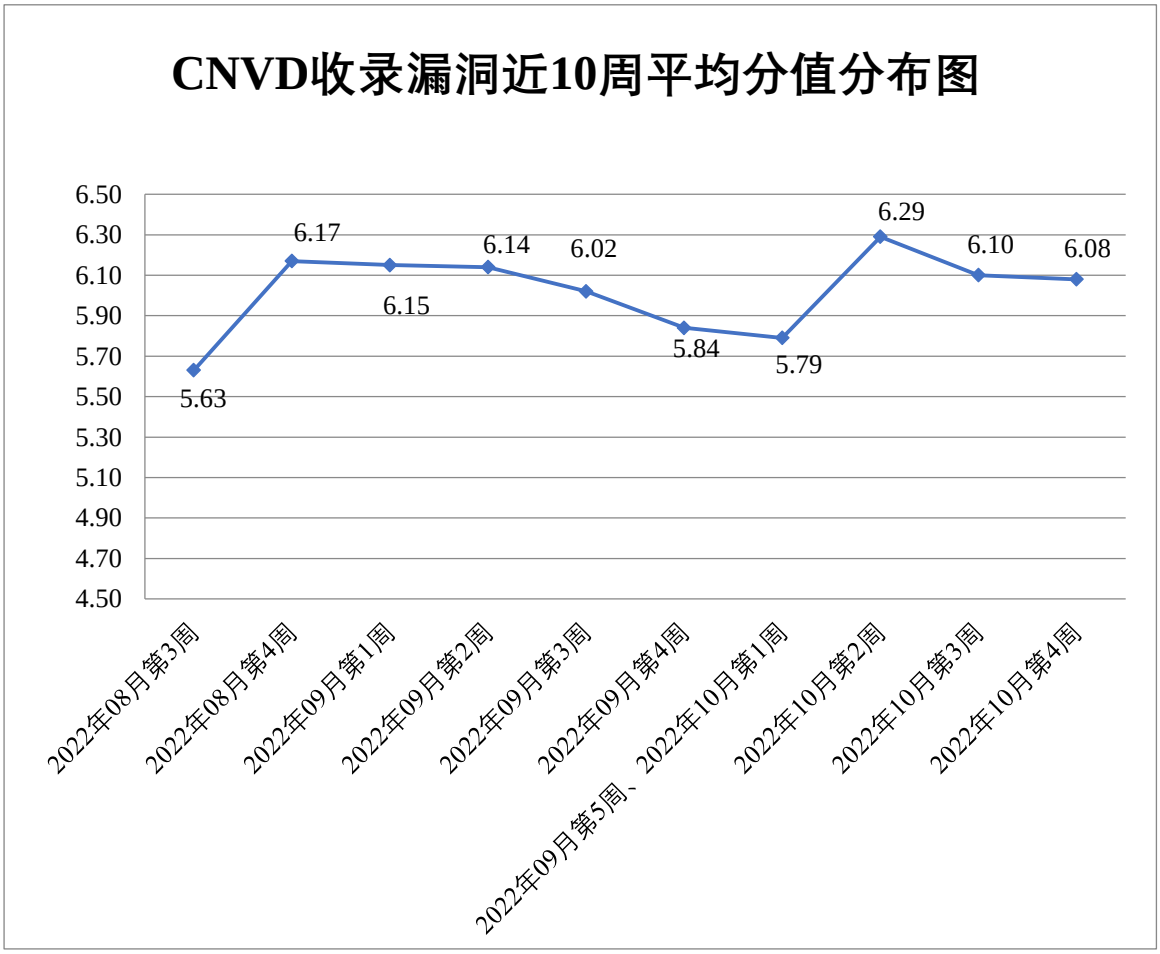

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 28 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 816 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 172 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 69 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：

浙江浙大中控信息技术有限公司、用友网络科技股份有限公司、西安新软信息科技有限公司、武汉岩海工程技术有限公司、武汉理工光科股份有限公司、完美世界征奇（上海）多媒体科技有限公司、苏州中祭网信息科技有限公司、苏州祥云平台信息技术有限公司、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、深圳市思迅软件股份有限公司、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、深圳市博思协创网络科技有限公司、深圳飞思安诺网络技术有限公司、上海展盟网络科技有限公司、上海禹亮信息科技有限公司、上海优度宽带科技有限公司、上海博达数据通信有限公司、闪捷信息科技有限公司、山东中维世纪科技股份有限公司、山东中创软件商用中间件股份有限公司、山东金钟科技集团股份有限公司、厦门四信通信科技有限公司、厦门四联信息技术有限公司、任子行网络技术股份有限公司、青果软件集团有限公司、麒麟软件有限公司、南京云网汇联软件技术有限公司、迈普通信技术股份有限公司、雷蛇技术开发（深圳）有限公司、江苏健科软件有限公司、佳能（中国）有限公司、佳乐科技有限责任公司、吉翁电子（深圳）有限公司、华硕电脑（上海）有限公司、宏脉信息技术（广州）股份有限公司、广州网易计算机系统有限公司、广州市品高软件股份有限公司、广州几维信息科技有限公司、广州红帆科技有限公司、广州鼎甲计算机科技有限公司、广东全程云科技有限公司、广东金砖天网信息科技有限公司、大连华天软件有限公司、成都傲梅科技有限公司、北京中科网威信息技术有限公司、北京中盾安信科技发展有限公司、北京致远互联软件股份有限公司、北京云帆互联科技有限公司、北京星网锐捷网络技术有限公司、北京万户网络技术有限公司、北京数字政通科技股份有限公司、北京杰控科技有限公司、北京和欣运达科技有限公司、北京格林威尔科技发展有限公司、北京东方通科技股份有限公司、北京大爱惠民医疗科技股份有限公司、北京北信源软件股份有限公司、北京北大方正电子有限公司、北京百卓网络技术有限公司和北京安华金和科技有限公司。

本周，CNVD 发布了《Oracle 发布 2022 年 10 月的安全公告》、《F5 发布 2022 年

10 月季度安全通告》。详情参见 CNVD 网站公告内容。

https://www.cnvd.org.cn/webinfo/show/8221

https://www.cnvd.org.cn/webinfo/show/8226

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、新华三技术有限公司、安天科技集团股份有限公司、深信服科技股份有限公司、北京数字观星科技有限公司等单位报送公开收集的漏洞数量较多。远江盛邦（北京）网络安全科技股份有限公司、南京众智维信息科技有限公司、西安四叶草信息技术有限公司、北京升鑫网络科技有限公司、河南信安世纪科技有限公司、奇安星城网络安全运营服务（长沙）有限公司、北京山石网科信息技术有限公司、杭州迪普科技股份有限公司、山东云天安全技术有限公司、长春嘉诚信息技术股份有限公司、浙江木链物联网科技有限公司、苏州棱镜七彩信息科技有限公司、河南东方云盾信息技术有限公司、广东唯顶信息科技股份有限公司、山东新潮信息技术有限公司、北京华顺信安信息技术有限公司、杭州默安科技有限公司、安徽锋刃信息科技有限公司、浙江大华技术股份有限公司、北京雪诺科技有限公司、上海纽盾科技股份有限公司、北京云科安信科技有限公司（Seraph 安全实验室）、北京冠程科技有限公司、联通数字科技有限公司、中通服创发科技有限责任公司、江苏保旺达软件技术有限公司、中国工程物理研究院计算机应用研究所、北京安帝科技有限公司、西安交大捷普网络科技有限公司、亚信科技（成都）有限公司、北京远禾科技有限公司、上海迅御安全科技有限公司、山石网科通信技术股份有限公司、云南联创网安科技有限公司、重庆都会信息科技有限公司、成都安美勤信息技术股份有限公司、上海齐同信息科技有限公司、南京节点安全技术有限公司、北京微步在线科技有限公司、有度网络安全技术有限公司、新疆海狼科技有限公司及其他个人白帽子向 CNVD 提交了 13636 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）、奇安信网神（补天平台）、上海交大和三六零数字安全科技集团有限公司向 CNVD 共享的白帽子报送的 11540 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
斗象科技（漏洞盒子）	5755	5755
奇安信网神（补天平台）	4836	4836
上海交大	790	790
北京神州绿盟科技有限公司	362	9

新华三技术有限公司	329	0
远江盛邦（北京）网络安全科技股份有限公司	281	281
安天科技集团股份有限公司	280	0
南京众智维信息科技有限公司	273	273
深信服科技股份有限公司	240	0
三六零数字安全科技集团有限公司	159	159
北京数字观星科技有限公司	127	0
恒安嘉新（北京）科技股份公司	114	2
西安四叶草信息技术有限公司	90	90
北京启明星辰信息安全技术有限公司	81	23
天津市国瑞数码安全系统股份有限公司	59	0
杭州安恒信息技术股份有限公司	49	11
中国电信集团系统集成有限责任公司	30	0
北京知道创宇信息技术有限公司	30	0
阿里云计算有限公司	20	0
卫士通信息产业股份有限公司	15	15
北京长亭科技有限公司	10	10
南京联成科技发展股份有限公司	8	8

内蒙古云科数据服务股份有限公司	6	6
北京天融信网络安全技术有限公司	3	3
深圳市腾讯计算机系统有限公司（玄武实验室）	1	1
北京升鑫网络科技有限公司	83	83
河南信安世纪科技有限公司	65	65
奇安星城网络安全运营服务（长沙）有限公司	59	59
北京山石网科信息技术有限公司	56	56
杭州迪普科技股份有限公司	27	6
山东云天安全技术有限公司	17	17
长春嘉诚信息技术股份有限公司	15	15
浙江木链物联网科技有限公司	14	14
苏州棱镜七彩信息科技有限公司	13	13
河南东方云盾信息技术有限公司	13	13
广东唯顶信息科技股份有限公司	12	12
山东新潮信息技术有限公司	10	10
北京华顺信安信息技术有限公司	6	5
杭州默安科技有限公	6	6

司		
安徽锋刃信息科技有限公司	6	6
浙江大华技术股份有限公司	4	4
北京雪诺科技有限公司	3	3
上海纽盾科技股份有限公司	3	3
北京云科安信科技有限公司（Seraph 安全实验室）	3	3
北京冠程科技有限公司	2	2
联通数字科技有限公司	2	2
中通服创发科技有限责任公司	2	2
江苏保旺达软件技术有限公司	2	2
中国工程物理研究院计算机应用研究所	2	2
北京安帝科技有限公司	2	2
西安交大捷普网络科技有限公司	2	2
亚信科技（成都）有限公司	1	0
北京远禾科技有限公司	1	1
上海迅御安全科技有限公司	1	1
山石网科通信技术股份有限公司	1	1
云南联创网安科技有	1	1

限公司		
重庆都会信息科技有限公司	1	1
成都安美勤信息技术股份有限公司	1	1
上海齐同信息科技有限公司	1	1
南京节点安全技术有限公司	1	1
北京微步在线科技有限公司	1	1
有度网络安全技术有限公司	1	1
新疆海狼科技有限公司	1	1
CNCERT 贵州分中心	3	3
个人	943	943
报送总计	15335	13636

本周漏洞按类型和厂商统计

本周，CNVD 收录了 508 个漏洞。WEB 应用 247 个，应用程序 124 个，网络设备（交换机、路由器等网络端设备）63 个，操作系统 41 个，智能设备（物联网终端设备）27 个，安全产品 4 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
WEB 应用	247
应用程序	124
网络设备（交换机、路由器等网络端设备）	63
操作系统	41
智能设备（物联网终端设备）	27
安全产品	4
数据库	2

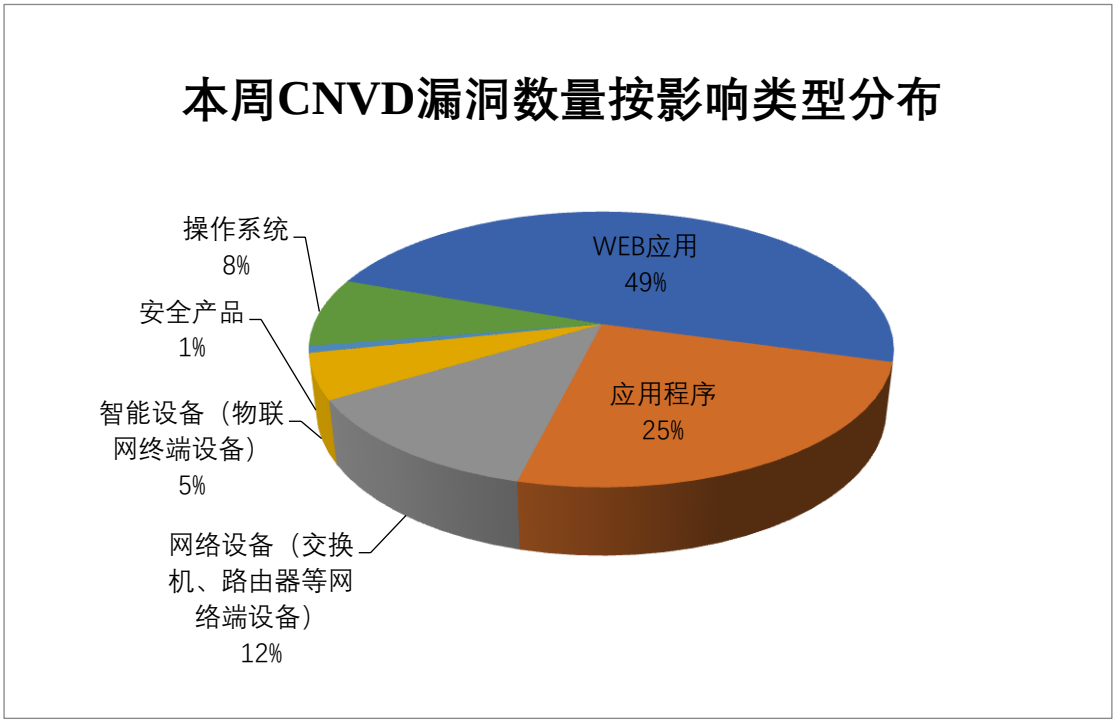

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Samsung、WordPress、H3C 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	Samsung	31	6%
2	WordPress	23	5%
3	H3C	17	3%
4	Apple	14	3%
5	Libtiff	14	3%
6	Microsoft	11	2%
7	F5	10	2%
8	Apache	9	2%
9	Linux	9	2%
10	其他	370	72%

本周行业漏洞收录情况

本周，CNVD 收录了 42 个电信行业漏洞，68 个移动互联网行业漏洞，3 个工控行业漏洞（如下图所示）。其中，“Samsung Galaxy Store 输入验证错误漏洞（CNVD-2022-70731）、Apple iPadOS 和 Apple iOS 缓冲区溢出漏洞、Google Android 代码执行漏洞（CNVD-2022-71986）”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/

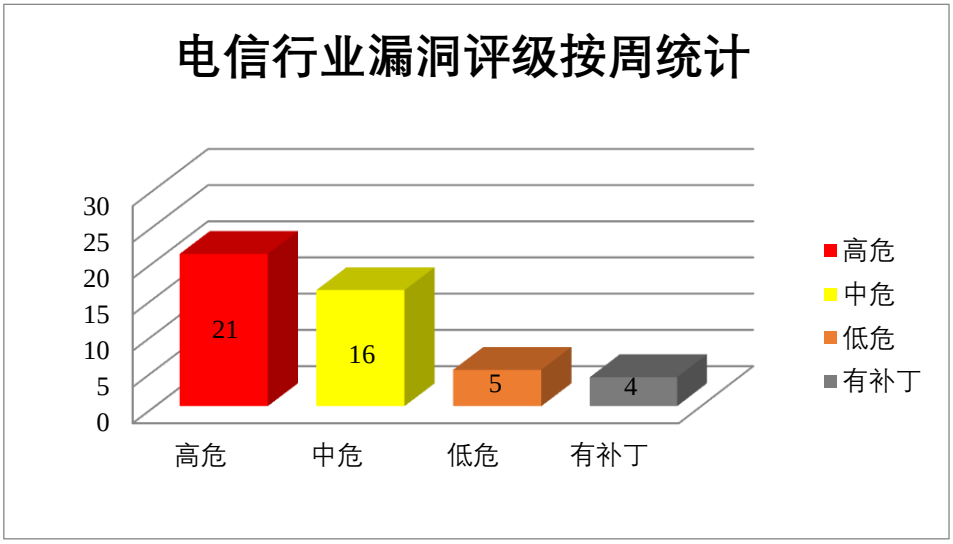

图 3 电信行业漏洞统计

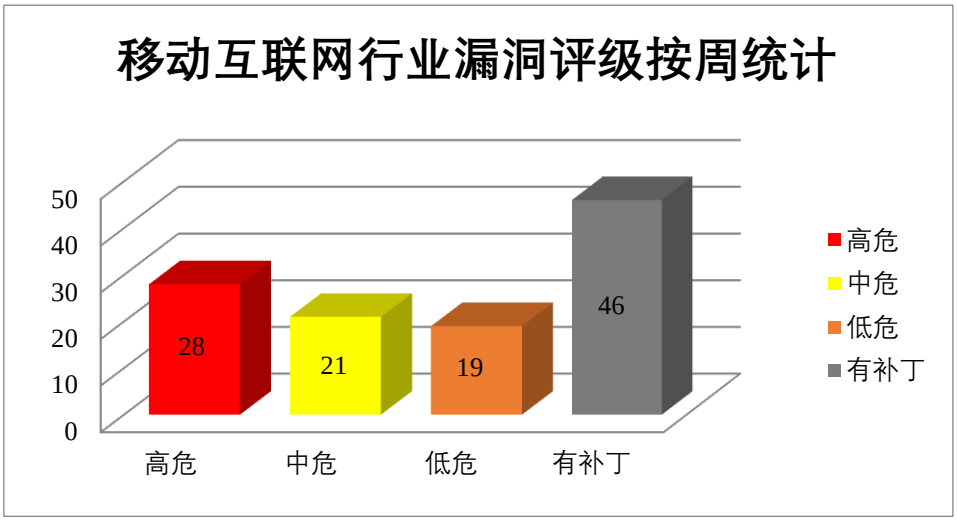

图 4 移动互联网行业漏洞统计

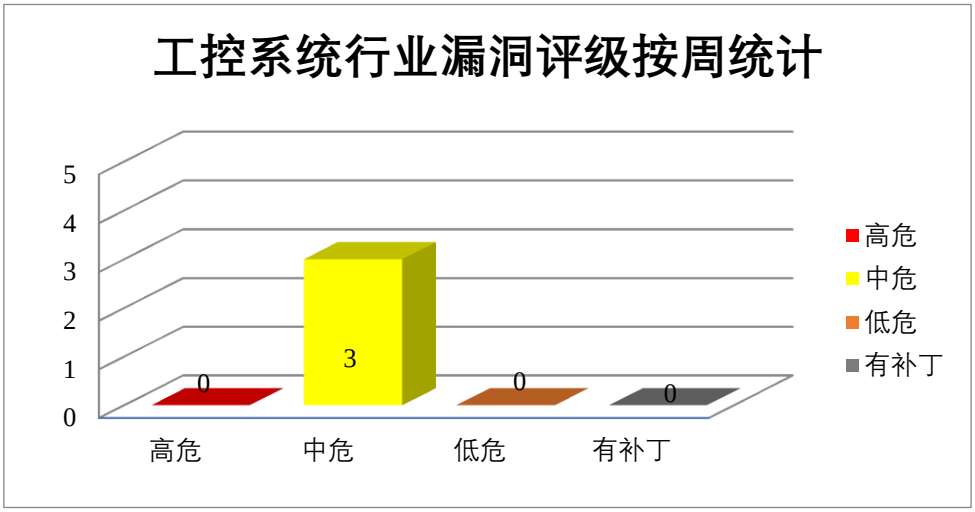

图 5 工控系统行业漏洞统计

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，攻击者可利用增加磁盘利用率，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 XML 外部实体注入漏洞（CNVD-2022-70618）、F5 BIG-IP 代码问题漏洞（CNVD-2022-70623）、F5 BIG-IP 配置文件漏洞、F5 BIG-IP 资源管理错误漏洞（CNVD-2022-70619、CNVD-2022-70626）、F5 BIG-IP AFM 资源管理错误漏洞、F5 BIG-IP 代码问题漏洞（CNVD-2022-70624、CNVD-2022-70627）。其中，“F5 BIG-IP 代码问题漏洞（CNVD-2022-70627）”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-2022-70618

https://www.cnvd.org.cn/flaw/show/CNVD-2022-70623

https://www.cnvd.org.cn/flaw/show/CNVD-2022-70622

https://www.cnvd.org.cn/flaw/show/CNVD-2022-70619

https://www.cnvd.org.cn/flaw/show/CNVD-2022-70626

https://www.cnvd.org.cn/flaw/show/CNVD-2022-70625

https://www.cnvd.org.cn/flaw/show/CNVD-2022-70624

https://www.cnvd.org.cn/flaw/show/CNVD-2022-70627

2、Google 产品安全漏洞

Google Android 是美国谷歌(Google)公司的一套以 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，在系统上执行任意代码，造成拒绝服务。

CNVD 收录的相关漏洞包括：Google Android 信息泄露漏洞（CNVD-2022-71979、CNVD-2022-71980、CNVD-2022-71982、CNVD-2022-71985）、Google Android 拒绝服务漏洞（CNVD-2022-71981）、Google Android 代码执行漏洞（CNVD-2022-71983、CNVD-2022-71984、CNVD-2022-71986）。其中，除“Google Android 拒绝服务漏洞（CNVD-2022-71981）、Google Android 信息泄露漏洞（CNVD-2022-71985）”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-2022-71979
https://www.cnvd.org.cn/flaw/show/CNVD-2022-71980
https://www.cnvd.org.cn/flaw/show/CNVD-2022-71981
https://www.cnvd.org.cn/flaw/show/CNVD-2022-71982
https://www.cnvd.org.cn/flaw/show/CNVD-2022-71983
https://www.cnvd.org.cn/flaw/show/CNVD-2022-71984
https://www.cnvd.org.cn/flaw/show/CNVD-2022-71985
https://www.cnvd.org.cn/flaw/show/CNVD-2022-71986

3、 Apple 产品安全漏洞

Apple macOS Monterey 是美国苹果（Apple）公司的用于麦金塔桌面操作系统 mac OS 的第 18 个主要版本。Apple Safari 是一款 Web 浏览器，是 Mac OS X 和 iOS 操作系统附带的默认浏览器。Apple iOS 是一套为移动设备所开发的操作系统。Apple iPadOS 是一套用于 iPad 平板电脑的操作系统。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞提升权限，在目标系统上执行任意代码等。

CNVD 收录的相关漏洞包括：Apple macOS Monterey 缓冲区溢出漏洞（CNVD-2022-71990）、Apple macOS Safari 缓冲区溢出漏洞、Apple macOS Monterey Spotlight 权限许可和访问控制问题漏洞、Apple macOS Monterey 缓冲区溢出漏洞、Apple iOS and iPadOS GPU 驱动程序代码注入漏洞、Apple iOS and iPadOS GPU 驱动程序缓冲区溢出漏洞、Apple iOS and iPadOS 输入验证错误漏洞、Apple iOS and iPadOS WebKit 缓冲区溢出漏洞。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-2022-71990
https://www.cnvd.org.cn/flaw/show/CNVD-2022-71988
https://www.cnvd.org.cn/flaw/show/CNVD-2022-71993
https://www.cnvd.org.cn/flaw/show/CNVD-2022-71992

https://www.cnvd.org.cn/flaw/show/CNVD-2022-71991

https://www.cnvd.org.cn/flaw/show/CNVD-2022-71999

https://www.cnvd.org.cn/flaw/show/CNVD-2022-71998

https://www.cnvd.org.cn/flaw/show/CNVD-2022-71996

4、Microsoft 产品安全漏洞

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 DNS Server 是其中的一个 DNS（域名系统）服务器。Microsoft Windows Cluster Shared Volume (CSV) 是美国微软（Microsoft）公司的一项功能。Microsoft HEVC Video Extensions 是美国微软（Microsoft）公司的一个视频扩展应用程序。该应用使计算机和设备可以读取高效视频编码或 HEVC 视频。Microsoft Windows Defender 是美国微软（Microsoft）公司的一套 Windows 系统附带的防病毒软件。Microsoft Windows Fax services 是美国微软（Microsoft）公司的一个功能组件服务。用于指定传真的设置，包括如何发送，接收，查看和打印。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，在系统上执行任意代码，造成拒绝服务。

CNVD 收录的相关漏洞包括：Microsoft Windows DNS Server 远程代码执行漏洞（CNVD-2022-71743、CNVD-2022-71975）、Microsoft Windows Cluster Shared Volume (CSV) 拒绝服务漏洞、Microsoft HEVC Video Extensions 远程代码执行漏洞（CNVD-2022-71765）、Microsoft Windows Defender 拒绝服务漏洞、Microsoft Windows DiskUsage.exe 远程代码执行漏洞、Microsoft Windows DNS Server 信息泄露漏洞、Microsoft Windows Fax Compose Form 远程代码执行漏洞。其中，“Microsoft Windows DNS Server 远程代码执行漏洞（CNVD-2022-71743、CNVD-2022-71975）、Microsoft HEVC Video Extensions 远程代码执行漏洞（CNVD-2022-71765）”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-2022-71743

https://www.cnvd.org.cn/flaw/show/CNVD-2022-71764

https://www.cnvd.org.cn/flaw/show/CNVD-2022-71765

https://www.cnvd.org.cn/flaw/show/CNVD-2022-71972

https://www.cnvd.org.cn/flaw/show/CNVD-2022-71973

https://www.cnvd.org.cn/flaw/show/CNVD-2022-71974

https://www.cnvd.org.cn/flaw/show/CNVD-2022-71975

https://www.cnvd.org.cn/flaw/show/CNVD-2022-71976

5、Avantune Genialcloud ProJ 跨站脚本漏洞

Avantune Genialcloud ProJ 是加拿大 Avantune 公司的一个基于云的 ERP 平台。本周，Avantune Genialcloud ProJ 被披露存在跨站脚本漏洞。攻击者可利用该漏洞通过精

心设计的有效负载注入和执行任意 Web 脚本或 HTML。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-2022-71647

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-2022-70613	Siemens Siveillance Video Mobile Server 身份验证绕过漏洞	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://cert-portal.siemens.com/productcert/html/ssa-640732.html
CNVD-2022-70627	F5 BIG-IP 代码问题漏洞（CNVD-2022-70627）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://support.f5.com/csp/article/K57111075
CNVD-2022-70755	Samsung UWB stack 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://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=3
CNVD-2022-70763	WordPress Block Bad Bots plugin SQL 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://wpscan.com/vulnerability/e00b2946-15e5-4458-9b13-2e272630a36f
CNVD-2022-71115	Tongda2000 SQL 注入漏洞（CNVD-2022-71115）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.tongda2000.com/download/p2019.php?F=baidu_natural&K=
CNVD-2022-71112	Cybonet PineApp Mail Relay SQL 注入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：http://www.pineapp.com/en/
CNVD-2022-71401	Apache Cordova 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://www.apache.org/
CNVD-2022-71994	Apple iPadOS 和 Apple iOS 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://support.apple.com/en-us/HT213346
CNVD-2022-70731	Samsung Galaxy Store 输入验证错误漏洞（CNVD-2022-	高	厂商已发布了漏洞修复程序，请及时关注更新：

	70731）		https://security.samsungmobile.com/securityUpdate.smsb?year=2022&month=7
CNVD-2022-71509	Apple iOS and iPadOS 任意代码执行漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://support.apple.com/en-us/HT213489

小结：本周，F5 产品被披露存在多个漏洞，攻击者可利用增加磁盘利用率，在 BIG-IP 系统上造成拒绝服务等。此外，Google、Apple、Microsoft 等多款产品被披露存在多个漏洞，攻击者可利用漏洞提升权限，获取敏感信息，在系统上执行任意代码，造成拒绝服务等。另外，Avantune Genialcloud ProJ 被披露存在跨站脚本漏洞。攻击者可利用该漏洞通过精心设计的有效负载注入和执行任意 Web 脚本或 HTML。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、BloofoxCms SQL 注入漏洞

验证描述

BloofoxCms 是一个基于 Php 的文本内容管理系统。

BloofoxCms 0.5.1（包含）至 0.5.2.1（包含）版本存在 SQL 注入漏洞，该漏洞源于以下参数“URLs,lang_id,tmpl_id,mod_rewrite,eta_doctype,meta_charset,default_group,page group”缺少对外部输入 SQL 语句的验证。攻击者可利用该漏洞执行非法 SQL 命令窃取数据库敏感数据。

验证信息

POC 链接：https://github.com/alexlang24/bloofoxCMS/issues/13

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2022-71120

信息提供者

新华三技术有限公司

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. 苹果修复了被利用的 iOS、iPadOS 零日漏洞 (CVE-2022-42827)

苹果公司今年第九次发布了针对零日漏洞(CVE-2022-42827)的修复程序，该漏洞可

被攻击者利用危害 iPhone 安全。

参考链接：https://www.helpnetsecurity.com/2022/10/25/cve-2022-42827/

2. Orca Security 披露 Azure SFX 漏洞 FabriXss 细节

据外媒报道，Orca Security 发现了 Service Fabric Explorer(SFX)中的漏洞 FabriXss (CVE-2022-35829)。该漏洞可被用来获得完整的管理员权限并劫持 Azure Service Fabric 集群。

参考链接：https://www.anquanke.com/post/id/282019

关于 CNVD

国家信息安全漏洞共享平台（China National Vulnerability Database，简称 CNVD）是由 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国家网络安全漏洞库，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，是我国计算机网络应急处理体系中的牵头单位。

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