国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2022 年 03 月 14 日-2022 年 03 月 20 日 **2022 年第 11 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 576 个，其中高危漏洞 172 个、中危漏洞 340 个、低危漏洞 64 个。漏洞平均分值为 5.81。本周收录的漏洞中，涉及 0day 漏洞 289 个（占 50%），其中互联网上出现“Snipe-IT 跨站脚本漏洞（CNVD-2022-19845）、PeteReport 跨站请求伪造漏洞”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 4022 个，与上周（4325 个）环比减少 7%。

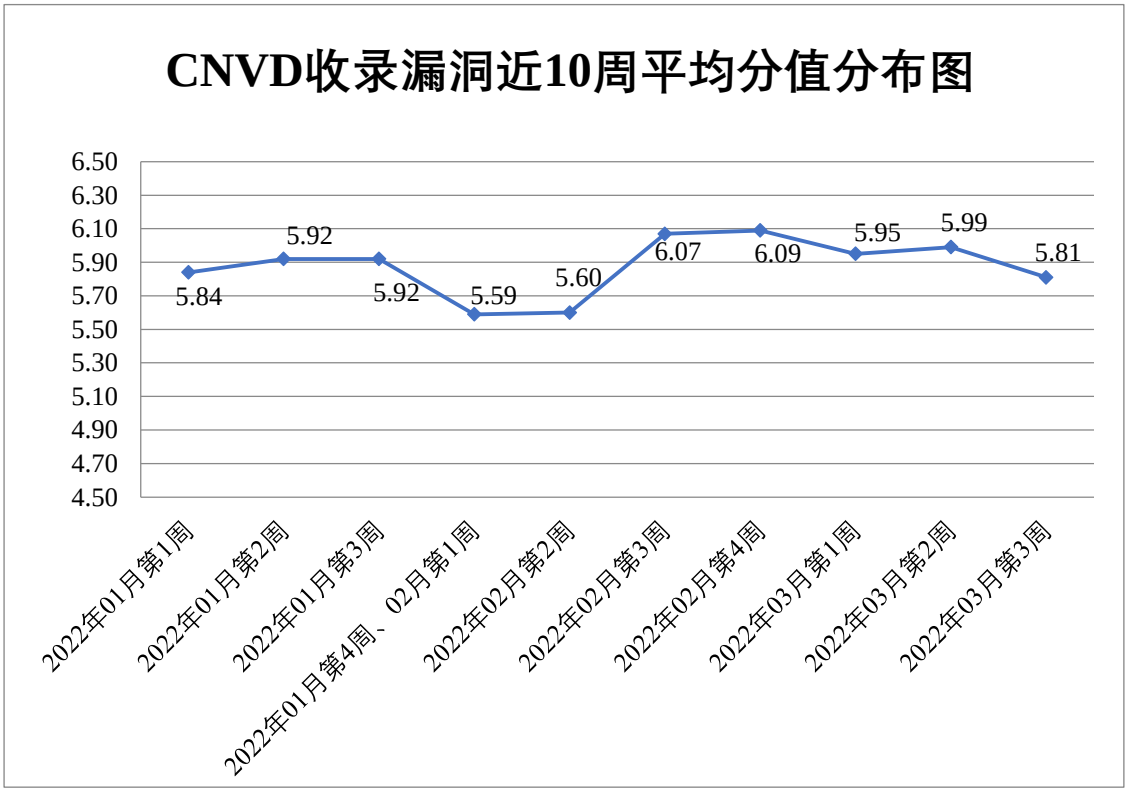

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 59 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 690 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 96 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 61 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：

遵义欣腾达信息技术有限公司、淄博闪灵网络科技有限公司、逐鹿科技有限公司上海分公司、珠海派诺科技股份有限公司、珠海金山办公软件有限公司、中新网络信息安全股份有限公司、中科博华信息科技有限公司、郑州天迈科技股份有限公司、正方软件股份有限公司、浙江浙大中控信息技术有限公司、长沙友点软件科技有限公司、漳州豆壳网络科技有限公司、友讯电子设备（上海）有限公司、兄弟（中国）商业有限公司、暇光软件科技（上海）有限公司、武汉神州数码云科网络技术有限公司、武汉达梦数据库股份有限公司、温州互引信息技术有限公司、微软（中国）有限公司、天津南大通用数据技术股份有限公司、太原迅易科技有限公司、索尼（中国）有限公司、苏州同牧网络科技有限公司、苏州科达科技股份有限公司、四创科技有限公司、四川迅睿云软件开发有限公司、深圳小信科技有限公司、深圳市迅雷网络技术有限公司、深圳市深海捷科技有限公司、深圳市明源云科技有限公司、深圳市朗驰欣创科技股份有限公司、深圳市科迈通讯技术有限公司、深圳市吉祥腾达科技有限公司、深圳市和为顺网络技术有限公司、深圳市博思协创网络科技有限公司、深圳市必联电子有限公司、深圳飞思安诺网络技术有限公司、深一科技集团有限公司、上海卓卓网络科技有限公司、上海银狐信息科技有限公司、上海七牛信息技术有限公司、上海脉信网络科技有限公司、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、上海二三四五网络科技有限公司、上海创图网络科技股份有限公司、上海贝锐信息科技股份有限公司、熵基科技股份有限公司、陕西汉投中小企业金融服务有限公司、山石网科通信技术股份有限公司、山脉科技股份有限公司、山东资略信息技术有限公司、厦门科汛软件有限公司、厦门科拓通讯技术股份有限公司、群晖网络科技（上海）有限公司、青岛极光软件科技有限公司、南京致汇达网络科技有限公司、南京数旗科技有限公司、南京埃斯顿自动化股份有限公司、灵宝简好网络科技有限公司、联奕科技股份有限公司、吉翁电子（深圳）有限公司、惠普贸易（上海）有限公司、淮南市银泰软件科技有限公司、河南硕朗通讯有限公司、杭州易软共创网络科技有限公司、杭州联创信息技术有限公司、杭州海康威视数字技术股份有限公司、杭州飞致云信息科技有限公司、杭州当虹科技股份有限公司、瀚高基础软件股份有限公司、海南赞赞网络科技有限公司、广州市动景计算机科技有限公司、广州鲁邦通物联网科技股份有限公司、广州巨杉软件开发有限公司、广州红帆科技有限公司、

广州恒企教育科技有限公司、广州好象科技有限公司、广西金中软件集团有限公司、广联达科技股份有限公司、福州网钛软件科技有限公司、福建银达汇智信息科技股份有限公司、福建升腾资讯有限公司、烽火通信科技股份有限公司、东芝（中国）有限公司、东华医为科技有限公司、东华软件股份公司、大连华天软件有限公司、北京字节跳动科技有限公司、北京中庆纳博信息技术有限公司、北京亚控科技发展有限公司、北京星网锐捷网络技术有限公司、北京五指互联科技有限公司、北京通达信科科技有限公司、北京人大金仓信息技术股份有限公司、北京平凯星辰科技发展有限公司、北京派网软件有限公司、北京京东叁佰陆拾度电子商务有限公司、北京慧图科技（集团）股份有限公司、北京超图软件股份有限公司、北京百卓网络技术有限公司、安徽中技国医医疗科技有限公司、安徽省科大奥锐科技有限公司、爱普生（中国）有限公司、阿里巴巴集团安全应急响应中心、腾讯安全应急响应中心、易贝 CMS、信呼、zzcms、Yamaha Corporation、VyOS、Vmware、The PostgreSQL Global Development Group、The Apache Software Foundation、SonicWall、SemCms、SchoolCMS、PingCAP、PHPMyWind、Notable、MuYuCMS、Geovision、ForU CMS、emlog、DrayTek Corp.、Dynacolor, Inc.和 Adobe。

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，新华三技术有限公司、安天科技集团股份有限公司、北京天融信网络安全技术有限公司、北京神州绿盟科技有限公司、杭州安恒信息技术股份有限公司等单位报送公开收集的漏洞数量较多。重庆都会信息科技有限公司、长春嘉诚信息技术股份有限公司、杭州默安科技有限公司、北京山石网科信息技术有限公司、江苏保旺达软件技术有限公司、南京树安信息技术有限公司、贵州多彩宝互联网服务有限公司、山东云天安全技术有限公司、华鲁数智信息技术（北京）有限公司、开元华创科技（集团）有限公司、星云博创科技有限公司、上海见形信息科技有限公司、天津偕行科技有限公司、北京安华金和科技有限公司、武汉安域信息安全技术有限公司、深圳昂楷科技有限公司、贵州泰若数字科技有限公司、河南灵创电子科技有限公司、上海纽盾科技股份有限公司、博智安全科技股份有限公司、河南信安世纪科技有限公司、任子行网络技术股份有限公司、上海市信息安全测评认证中心、思而听网络科技有限公司、内蒙古洞明科技有限公司、广西等保安全测评有限公司、杭州美创科技有限公司、天津启明星辰信息技术有限公司、苏州棱镜七彩信息科技有限公司、交通运输信息安全中心有限公司（TISEC 洪椒战队）、广西塔易信息技术有限公司、武汉非尼克斯软件技术有限公司、广州安亿信软件科技有限公司、北京冠程科技有限公司、南京禾盾信息科技有限公司及其他个人白帽子向 CNVD 提交了 4022 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 2104 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）	1462	1462
新华三技术有限公司	487	0
上海交大	458	458
安天科技集团股份有限公司	212	0
奇安信网神（补天平台）	184	184
北京天融信网络安全技术有限公司	134	34
北京神州绿盟科技有限公司	127	0
杭州安恒信息技术股份有限公司	110	38
远江盛邦（北京）网络安全科技股份有限公司	98	98
北京数字观星科技有限公司	94	0
恒安嘉新（北京）科技股份公司	92	0
西安四叶草信息技术有限公司	88	88
北京启明星辰信息安全技术有限公司	66	9
天津市国瑞数码安全系统股份有限公司	56	0
深信服科技股份有限公司	39	0
中国电信集团系统集成有限责任公司	30	0
南京众智维信息科技有限公司	26	26
内蒙古云科数据服务	18	18

股份有限公司		
南京铱迅信息技术股份有限公司	1	1
北京华顺信安科技有限公司	238	0
中国电信股份有限公司网络安全产品运营中心	140	0
亚信科技（成都）有限公司	88	0
重庆都会信息科技有限公司	44	44
长春嘉诚信息技术股份有限公司	31	31
杭州默安科技有限公司	27	27
杭州迪普科技股份有限公司	14	0
北京山石网科信息技术有限公司	11	11
江苏保旺达软件技术有限公司	10	10
南京树安信息技术有限公司	10	10
贵州多彩宝互联网服务有限公司	10	10
山东云天安全技术有限公司	9	9
华鲁数智信息技术（北京）有限公司	8	8
开元华创科技（集团）有限公司	6	6
星云博创科技有限公司	5	5
上海见形信息科技有	4	4

限公司		
天津偕行科技有限公司	4	4
北京安华金和科技有限公司	3	3
武汉安域信息安全技术有限公司	3	3
深圳昂楷科技有限公司	3	3
贵州泰若数字科技有限公司	3	3
河南灵创电子科技有限公司	3	3
上海纽盾科技股份有限公司	2	2
博智安全科技股份有限公司	2	2
河南信安世纪科技有限公司	2	2
任子行网络技术股份有限公司	1	1
上海市信息安全测评认证中心	1	1
思而听网络科技有限公司	1	1
内蒙古洞明科技有限公司	1	1
广西等保安全测评有限公司	1	1
杭州美创科技有限公司	1	1
天津启明星辰信息技术有限公司	1	1
苏州棱镜七彩信息科技有限公司	1	1

交通运输信息安全中心有限公司（TISEC 洪椒战队）	1	1
广西塔易信息技术有限公司	1	1
武汉非尼克斯软件技术有限公司	1	1
广州安亿信软件科技有限公司	1	1
北京冠程科技有限公司	1	1
南京禾盾信息科技有限公司	1	1
CNCERT 四川分中心	3	3
CNCERT 河北分中心	2	2
CNCERT 内蒙古分中心	1	1
个人	1386	1386
报送总计	5868	4022

本周漏洞按类型和厂商统计

本周，CNVD 收录了 576 个漏洞。WEB 应用 271 个，应用程序 130 个，网络设备（交换机、路由器等网络端设备）75 个，操作系统 44 个，智能设备（物联网终端设备）33 个，数据库 17 个，安全产品 6 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	271
应用程序	130
网络设备（交换机、路由器等网络端设备）	75
操作系统	44
智能设备（物联网终端设备）	33
数据库	17
安全产品	6

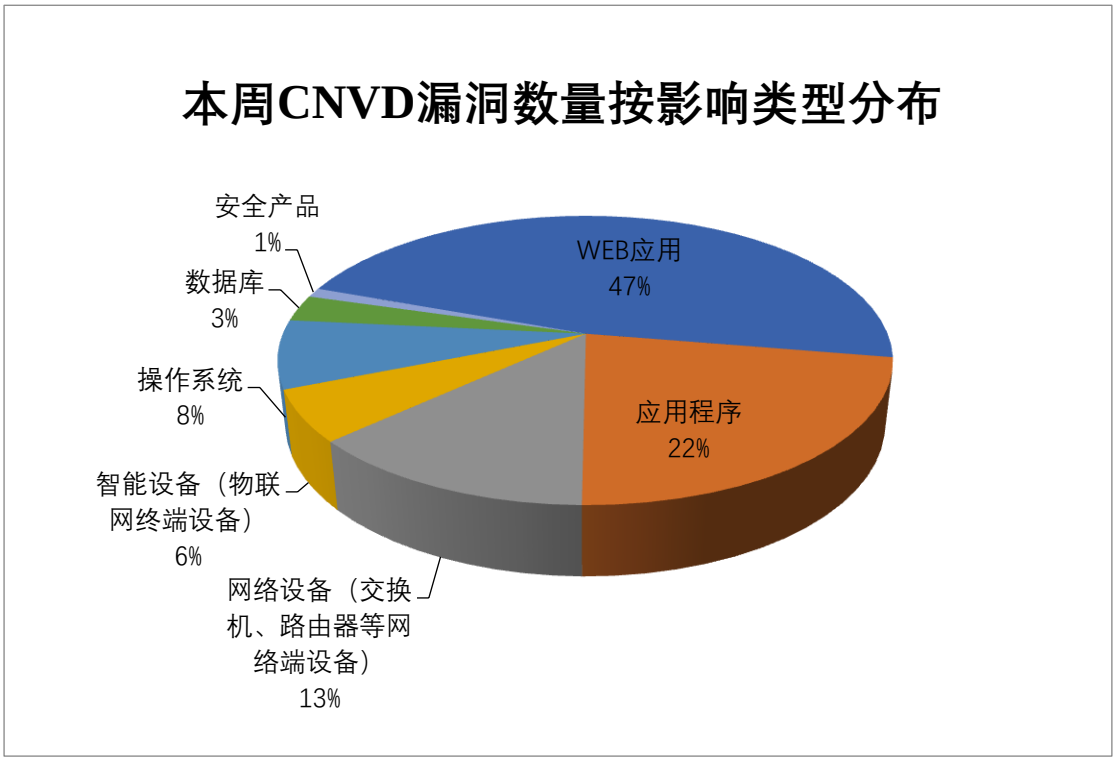

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 WordPress、Huawei、Google 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	WordPress	54	9%
2	Huawei	44	8%
3	Google	22	4%
4	ShowDoc	14	2%
5	D-Link	13	2%
6	DrayTek	12	2%
7	TP-LINK	12	2%
8	成都星锐蓝海网络科技有限公司	11	2%
9	luocms	10	2%
10	其他	384	67%

本周行业漏洞收录情况

本周，CNVD 收录了 51 个电信行业漏洞，26 个移动互联网行业漏洞，4 个工控行业漏洞（如下图所示）。其中，“D-Link DIR-859 缓冲区溢出漏洞、Tenda-AX3 缓冲区溢出漏洞、Huawei Emui 和 Magic UI 堆缓冲区溢出漏洞”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/

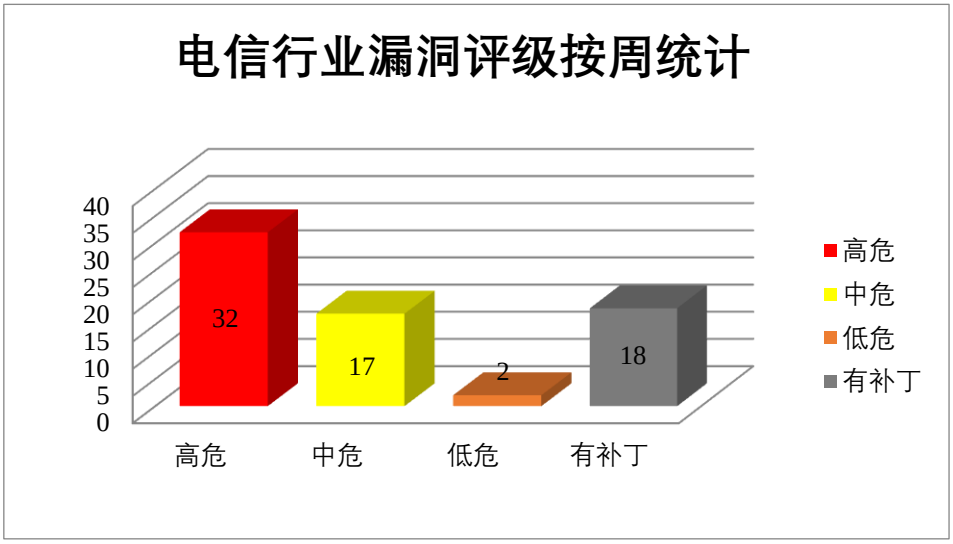

图 3 电信行业漏洞统计

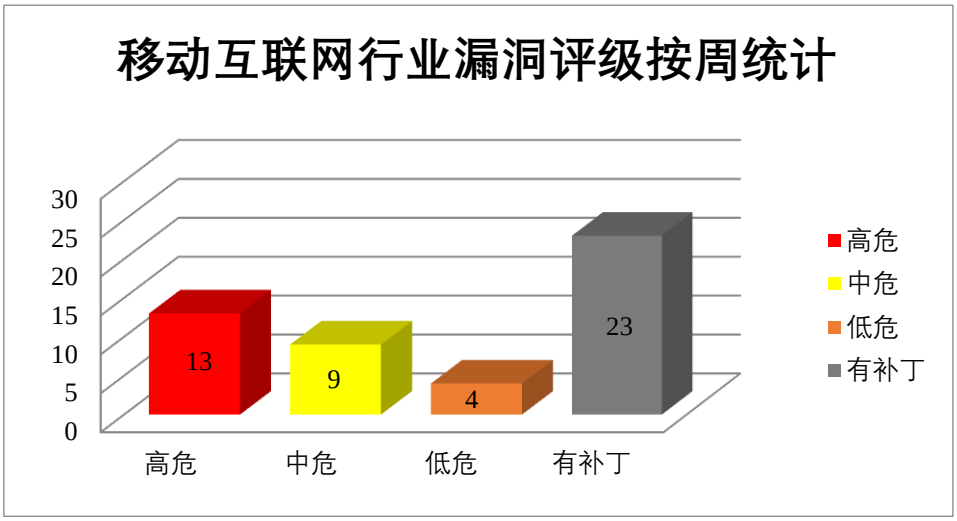

图 4 移动互联网行业漏洞统计

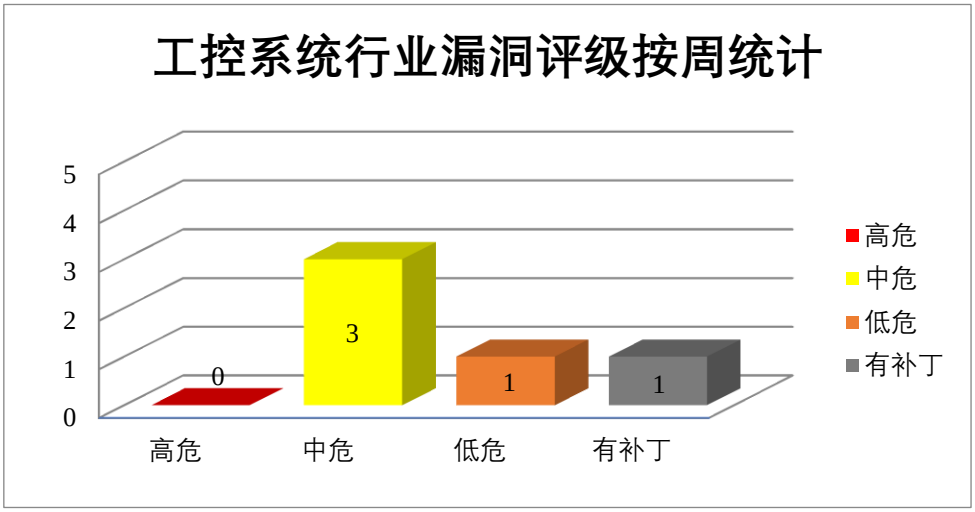

图 5 工控系统行业漏洞统计

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、 TP-Link 产品安全漏洞

TP-Link TL-WR886N 是中国普联（TP-Link）公司的一款路由器。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞使应用程序崩溃，在系统上执行任意代码。

CNVD 收录的相关漏洞包括：TP-Link TL-WR886N 缓冲区溢出漏洞（CNVD-2022-20072、CNVD-2022-20075、CNVD-2022-20074、CNVD-2022-20073、CNVD-2022-20077、CNVD-2022-20076）、TP-Link TL-WR886N 栈溢出漏洞（CNVD-2022-20081、CNVD-2022-20080）。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-2022-20072

https://www.cnvd.org.cn/flaw/show/CNVD-2022-20075

https://www.cnvd.org.cn/flaw/show/CNVD-2022-20074

https://www.cnvd.org.cn/flaw/show/CNVD-2022-20073

https://www.cnvd.org.cn/flaw/show/CNVD-2022-20077

https://www.cnvd.org.cn/flaw/show/CNVD-2022-20076

https://www.cnvd.org.cn/flaw/show/CNVD-2022-20081

https://www.cnvd.org.cn/flaw/show/CNVD-2022-20080

2、 Fortinet 产品安全漏洞

Fortinet FortiMail 是美国飞塔（Fortinet）公司的一套电子邮件安全网关产品。该产品提供电子邮件安全防护和数据保护等功能。Fortinet FortiWeb 是美国飞塔（Fortinet）公司的一款 Web 应用层防火墙，它能够阻断如跨站点脚本、SQL 注入、Cookie 中毒、s

chema 中毒等攻击的威胁，保证 Web 应用程序的安全性并保护敏感的数据库内容。Fortinet FortiExtender 是美国飞塔（Fortinet）公司的一款无线 WAN（广域网）扩展器设备。Fortinet FortiClientEms 是美国 Fortinet 公司的一个集中式中央管理系统。Fortinet FortiNAC 是美国飞塔（Fortinet）公司的一套网络访问控制解决方案。该产品主要用于网络访问控制和物联网安全防护。Fortinet FortiProxy SSL VPN 是美国 Fortinet 公司的一个应用软件。提供了一个入侵检测功能。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞对其进行解密并显示或更改其内容，在设备文件系统中执行任意文件和目录删除，通过特制的命令执行任意代码等。

CNVD 收录的相关漏洞包括：Fortinet FortiMail 跨站脚本漏洞（CNVD-2022-19073）、Fortinet FortiWeb 路径遍历漏洞（CNVD-2022-19072）、Fortinet FortiExtender 命令注入漏洞、Fortinet FortiClientEms 代码问题漏洞、Fortinet FortiNAC 权限提升漏洞、Fortinet FortiProxy SSL VPN 跨站请求伪造漏洞、Fortinet FortiWeb 缓冲区溢出漏洞（CNVD-2022-19074）、Fortinet FortiMail 加密问题漏洞。其中，“Fortinet FortiWeb 路径遍历漏洞（CNVD-2022-19072）、Fortinet FortiExtender 命令注入漏洞、Fortinet FortiClientEms 代码问题漏洞、Fortinet FortiNAC 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-2022-19073
https://www.cnvd.org.cn/flaw/show/CNVD-2022-19072
https://www.cnvd.org.cn/flaw/show/CNVD-2022-19071
https://www.cnvd.org.cn/flaw/show/CNVD-2022-19077
https://www.cnvd.org.cn/flaw/show/CNVD-2022-19076
https://www.cnvd.org.cn/flaw/show/CNVD-2022-19075
https://www.cnvd.org.cn/flaw/show/CNVD-2022-19074
https://www.cnvd.org.cn/flaw/show/CNVD-2022-19078

3、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。Magic Ui 是一款基于 Android 开发的移动端操作系统。Huawei eCNS280_TD 是中国华为（Huawei）公司的无线宽带集群系统的核心网设备。Huawei ESE620X vESS 是中国华为（Huawei）公司的一个虚拟企业服务控制器。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，绕过目标系统上的授权过程，导致拒绝服务等。

CNVD 收录的相关漏洞包括：Huawei Emui 和 Magic UI 缓冲区溢出漏洞（CNVD-2022-20296）、Huawei Emui 和 Magic UI 堆缓冲区溢出漏洞、Huawei Emui 和 Magic UI 拒绝服务漏洞（CNVD-2022-20298）、Huawei Emui 和 Magic UI 类型混淆漏洞、Huawei Emui 和 Magic UI IFAA 模块越界读取漏洞、Huawei Emui 和 Magic UI camera

组件空指针解引用漏洞、Huawei eCNS280_TD 和 ESE620X vESS 授权问题漏洞、Huawei eCNS280_TD 和 ESE620X vESS 越界读取漏洞。其中，“Huawei Emui 和 Magic UI 缓冲区溢出漏洞（CNVD-2022-20296）、Huawei Emui 和 Magic UI 堆缓冲区溢出漏洞、Huawei Emui 和 Magic UI 拒绝服务漏洞（CNVD-2022-20298）、Huawei Emui 和 Magic UI IFAA 模块越界读取漏洞”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-2022-20296
https://www.cnvd.org.cn/flaw/show/CNVD-2022-20295
https://www.cnvd.org.cn/flaw/show/CNVD-2022-20298
https://www.cnvd.org.cn/flaw/show/CNVD-2022-20297
https://www.cnvd.org.cn/flaw/show/CNVD-2022-20300
https://www.cnvd.org.cn/flaw/show/CNVD-2022-20305
https://www.cnvd.org.cn/flaw/show/CNVD-2022-20324
https://www.cnvd.org.cn/flaw/show/CNVD-2022-20323

4、Google 产品安全漏洞

Google Android Automotive Os 是美国谷歌（Google）公司的一种直接在车载硬件上运行的操作系统和平台。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，攻击者可利用漏洞获取敏感信息，绕过安全限制，在系统上执行任意代码或造成拒绝服务情况等。

CNVD 收录的相关漏洞包括：Google Android Automotive Os 信息泄露漏洞、Google Chrome 安全特征问题漏洞（CNVD-2022-20550）、Google Chrome GPU 代码执行漏洞（CNVD-2022-20554）、Google Chrome Mojo 整数溢出漏洞、Google Chrome Animation 代码执行漏洞、Google Chrome 安全特征问题漏洞（CNVD-2022-20551）、Google Chrome Tab Groups 缓冲区溢出漏洞、Google Chrome Webstore API 代码执行漏洞。其中，除“Google Android Automotive Os 信息泄露漏洞”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-2022-20539
https://www.cnvd.org.cn/flaw/show/CNVD-2022-20550
https://www.cnvd.org.cn/flaw/show/CNVD-2022-20554
https://www.cnvd.org.cn/flaw/show/CNVD-2022-20553
https://www.cnvd.org.cn/flaw/show/CNVD-2022-20552
https://www.cnvd.org.cn/flaw/show/CNVD-2022-20551
https://www.cnvd.org.cn/flaw/show/CNVD-2022-20557

https://www.cnvd.org.cn/flaw/show/CNVD-2022-20556

5、Tenda AX12 缓冲区溢出漏洞

Tenda AX12 是中国腾达（Tenda）公司的一款双频千兆 Wifi 6 无线路由器。本周，Tenda AX12 被披露存在缓冲区溢出漏洞。该漏洞源于函数 sub_422CE4 中包含堆栈缓冲区溢出。攻击者可利用该漏洞通过 strcpy 参数引发拒绝服务 (DoS)。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-2022-20581

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-2022-19829	WordPress WP User Frontend 插件 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/6d3eeba6-5560-4380-a6e9-f008a9112ac6
CNVD-2022-20097	MyBB 远程代码执行漏洞（CNVD-2022-20097）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/mybb/mybb/security/advisories/GHSA-876v-gwgh-w57f
CNVD-2022-20158	Tenda-AX3 缓冲区溢出漏洞	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.tenda.com.cn/default.html
CNVD-2022-20288	Huawei Emui 和 Magic UI video framework 堆缓冲区溢出漏洞（CNVD-2022-20288）	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/2022/3/
CNVD-2022-20502	Adobe Photoshop 缓冲区溢出漏洞（CNVD-2022-20502）	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/photoshop/apsb21-113.html
CNVD-2022-20504	Adobe Photoshop 缓冲区溢出漏洞（CNVD-2022-20504）	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/photoshop/apsb21-113.html
CNVD-2022-20507	showdoc .webmv 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://github.com/star7th/showdoc/commit/3caa32334db0c277b84e993ea

			ca2036f5d1dbef8
CNVD-2022-20555	Google Chrome ANGLE 代码执行漏洞（CNVD-2022-20555）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://chromereleases.googleblog.com/2022/02/stable-channel-update-for-desktop_14.html
CNVD-2022-20577	Microweber 远程代码执行漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/microweber/microweber/commit/867bdda1b4660b0795ad7f87ab5abe9e44b2b318
CNVD-2022-20579	Cobbler 授权问题漏洞（CNVD-2022-20579）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/cobbler/cobbler/commit/9044aa990a94752fa5bd5a24051adde099280bfa

小结：本周，TP-Link 产品被披露存在多个漏洞，攻击者可利用漏洞使应用程序崩溃，在系统上执行任意代码。此外，Fortinet、Huawei、Google 等多款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，绕过安全限制，在系统上执行任意代码，导致拒绝服务等。另外，Tenda AX12 被披露存在缓冲区溢出漏洞。攻击者可利用该漏洞通过 strcpy 参数引发拒绝服务 (DoS)。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、Snipe-IT 跨站脚本漏洞（CNVD-2022-19845）

验证描述

Snipe-IT 是一套开源 IT 资产/许可证管理系统。

Snipe-IT 存在跨站脚本漏洞，该漏洞源于 WEB 应用缺少对客户端数据的正确验证，攻击者可利用该漏洞执行客户端代码。

验证信息

POC 链接：https://huntr.dev/bounties/6dccc49e-3843-4a4a-b397-5c659e5f8bfe/

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2022-19845

信息提供者

哈尔滨安天科技集团股份有限公司

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. 加密库 OpenSSL/LibreSSL 发现一个可远程利用的漏洞

加密库 OpenSSL 发现了一个可远程利用的高危漏洞。计算模平方根的 BN_mod_sqrt()包含 bug 会导致无限循环，它能用于发动拒绝服务攻击。OpenSSL 项目释出了 OpenSSL 3.0.2 和 1.1.1n 修复了漏洞。

参考链接：https://www.solidot.org/story?sid=70959

2. dompdf 中未修补的 RCE 漏洞会影响 HTML 到 PDF 转换器

研究人员在“dompdf”（一种基于 php 的 HTML 到 PDF 的转换器）中发现了一个未修补的安全漏洞，如果该漏洞被成功利用，可能会导致某些配置中的远程代码被执行。

参考链接：https://www.freebuf.com/articles/325277.html

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