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 21 日-2022 年 03 月 27 日 **2022 年第 12 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 537 个，其中高危漏洞 180 个、中危漏洞 272 个、低危漏洞 85 个。漏洞平均分值为 5.84。本周收录的漏洞中，涉及 0day 漏洞 299 个（占 56%），其中互联网上出现“Pimcore 跨站脚本漏洞（CNVD-2022-22702）、CuppaCMS SQL 注入漏洞（CNVD-2022-22322）”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 4620 个，与上周（4022 个）环比增加 15%。

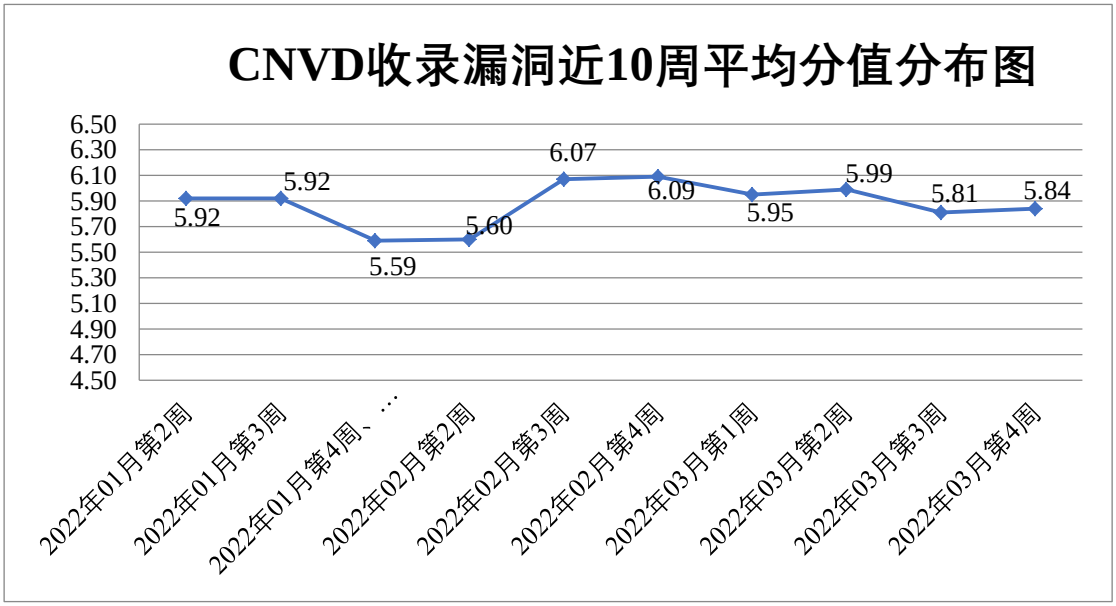

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 33 起，向基础电信企业通报漏洞事件 88 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 66 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 67 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：

卓豪（中国）技术有限公司、珠海金山办公软件有限公司、重庆中联信息产业有限责任公司、正方软件股份有限公司、浙江多普勒环保科技有限公司、浙江大华技术股份有限公司、长沙友点软件科技有限公司、长沙米拓信息技术有限公司、友讯电子设备（上海）有限公司、兄弟（中国）商业有限公司、新开普电子股份有限公司、暇光软件科技（上海）有限公司、武汉金同方科技有限公司、武汉烽火信息集成技术有限公司、温州互引信息技术有限公司、微软（中国）有限公司、台达电子企业管理（上海）有限公司、索尼（中国）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、四川广安爱众股份有限公司、世邦通信股份有限公司、深圳易达全球电子商务有限公司、深圳小信科技有限公司、深圳市中控生物识别技术有限公司、深圳市西迪特科技有限公司、深圳市网心科技有限公司、深圳市思迅软件股份有限公司、深圳市双梦科技有限公司、深圳市聚网捷科技有限公司、深圳市吉祥腾达科技有限公司、深圳市合信自动化技术有限公司、深圳市必联电子有限公司、上海卓卓网络科技有限公司、上海屹超信息技术有限公司、上海瑞策软件有限公司、上海米健信息技术有限公司、上海美赞美数码科技有限公司、上海肯特仪表股份有限公司、上海斐讯数据通信技术有限公司、上海缔安科技股份有限公司、上海碧海网络科技有限公司、熵基科技股份有限公司、商派软件有限公司、山洋电气（上海）贸易有限公司、山脉科技股份有限公司、山东山大华天软件有限公司、三星（中国）投资有限公司、赛马物联科技（宁夏）有限公司、青岛中瑞汽车服务有限公司、青岛海天炜业过程控制技术股份有限公司、麒麟软件有限公司、普联技术有限公司、宁波慕枫品牌策划有限公司、南宁安拓软件有限公司、南京易米云通网络科技有限公司、南京埃斯顿自动化股份有限公司、廊坊市极致网络科技有限公司、酷溜网（北京）科技有限公司、敬业集团有限公司、江西铭软科技有限公司、江苏天瑞仪器股份有限公司、江苏金智教育信息股份有限公司、济南唐丰信息科技有限公司、济南爱程网络科技有限公司、吉翁电子（深圳）有限公司、合肥图鸭信息科技有限公司、合肥奇乐网络科技有限公司、杭州智源电子有限公司、杭州益仕行信息技术有限公司、杭州雄伟科技开发股份有限公司、杭州千家网络有限公司、杭州海康威视数字技术股份有限公司、杭州冠航科技有限公司、杭州飞致云信息科技有限公司、哈尔滨伟成科技有限公司、桂林崇胜网络科技有限公司、广州中望龙腾软件股份有限公司、广州添富信息科技有限责任公司、广州市颖峰信息科技有限公司、广州市动景计算机科技有限公司、广州齐博网络科技有限公司、广联达科技股份有限公司、广东卓锐软件有限公司、观脉科技（北京）有限公司、福州网钛软件科技有限公司、福州木头软件有限公司、东芝（中国）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、成都万江港利科技股份有限公司、成都同飞科技有限责任公司、成都傲梅科技有限公司、畅捷通信息技术股份有限公司、北京字节跳动科技有限公司、北京中新天达科技有限公司、北京中科网威信息技术有限公司、北京致远互联软件股份有限公司、北京云网联科技有限公司、北京云帆互联科技有限公司、北京用友融联科技有限公司、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、北京网御星云信息技术有限公司、北京通达信科科技有限公司、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、北京擎企网络技术有限公司、北京派网软件有限公司、北京猎鹰安全科技有限公司、北京九思协同软件有限公司、北京金万维科技有限公司、北京金和网络股份有限公司、北京宏业超世纪科技有限公司、北京和信创天科技股份有限公司、北京东方通科技股份有限公司、北京百卓网络技术有限公司、北京爱奇艺科技有限公司、北大医疗信息技术有限公司、安科瑞电气股份有限公司、安徽容知日新科技股份有限公司、安徽科威网络科技有限公司、安徽富煌科技股份有限公司、阿里巴巴集团安全应急响应中心、涿鹿创梦网络工作室、新秀工作室、极路由、ZAVIO、yzmcms、The Apache Software Foundation、SonicWALL, Inc.、SeaCMS、Sapido Technology Inc、Realtek Semiconductor Corporation、Optilink Networks、NetSarang、Netis Systems、MuYucms、IRZ、Harbor、Grafana Labs、Geovision、Emlog、Elite Graphix、baigo Studio、Altran Group 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、杭州安恒信息技术股份有限公司、安天科技集团股份有限公司、北京神州绿盟科技有限公司、北京天融信网络安全技术有限公司等单位报送公开收集的漏洞数量较多。北京华顺信安科技有限公司、杭州默安科技有限公司、山东云天安全技术有限公司、内蒙古洞明科技有限公司、长春嘉诚信息技术股份有限公司、北京山石网科信息技术有限公司、墨菲未来科技（北京）有限公司、上海纽盾科技股份有限公司、南京树安信息技术有限公司、重庆都会信息科技有限公司、江苏保旺达软件技术有限公司、上海天存信息技术有限公司、山东泽鹿安全技术有限公司、山东新潮信息技术有限公司、广西等保安全测评有限公司、河南灵创电子科技有限公司、湖南中测网安信息技术有限公司、河南天祺信息安全技术有限公司、河南信安世纪科技有限公司、快页信息技术有限公司、广州百蕴启辰科技有限公司、深圳昂楷科技有限公司、苏州棱镜七彩信息科技有限公司、国网山东省电力公司、华鲁数智信息技术（北京）有限公司、南京禾盾信息科技有限公司、上海贝锐信息科技股份有限公司、厦门星舟科技有限公司、北京科技大学、上海上讯信息技术股份有限公司、开元华创科技集团、中国烟草总公司湖北省公司、武汉非尼克斯软件技术有限公司、广东蓝爵网络安全技术股份有限公司、思而听网络科技有限公司、浙江乾冠信息安全研究院、

北京机沃科技有限公司及其他个人白帽子向 CNVD 提交了 4620 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 2193 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
上海交大	983	983
斗象科技（漏洞盒子）	774	774
奇安信网神（补天平台）	436	436
新华三技术有限公司	317	0
杭州安恒信息技术股份有限公司	302	57
安天科技集团股份有限公司	228	4
北京神州绿盟科技有限公司	173	0
北京天融信网络安全技术有限公司	117	21
西安四叶草信息技术有限公司	115	115
北京数字观星科技有限公司	113	0
恒安嘉新（北京）科技股份公司	95	0
三六零数字安全科技集团有限公司	73	0
北京启明星辰信息安全技术有限公司	66	3
深信服科技股份有限公司	63	1
天津市国瑞数码安全系统股份有限公司	59	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	21	21

有限公司		
北京知道创宇信息技术股份有限公司	13	0
南京联成科技发展股份有限公司	11	11
远江盛邦（北京）网络安全科技股份有限公司	5	5
内蒙古云科数据服务股份有限公司	5	5
深圳市腾讯计算机系统有限公司（玄武实验室）	1	1
北京华顺信安科技有限公司	215	1
亚信科技（成都）有限公司	85	0
杭州默安科技有限公司	46	46
山东云天安全技术有限公司	40	40
内蒙古洞明科技有限公司	38	38
长春嘉诚信息技术股份有限公司	37	37
北京山石网科信息技术有限公司	34	34
墨菲未来科技（北京）有限公司	28	2
上海纽盾科技股份有限公司	26	26
南京树安信息技术有限公司	22	22
重庆都会信息科技有限公司	20	20

江苏保旺达软件技术有限公司	15	15
杭州迪普科技股份有限公司	14	0
上海天存信息技术有限公司	5	5
山东泽鹿安全技术有限公司	5	5
山东新潮信息技术有限公司	4	4
广西等保安全测评有限公司	4	4
河南灵创电子科技有限公司	3	3
湖南中测网安信息技术有限公司	3	3
河南天祺信息安全技术有限公司	2	2
河南信安世纪科技有限公司	2	2
快页信息技术有限公司	2	2
广州百蕴启辰科技有限公司	2	2
深圳昂楷科技有限公司	2	2
苏州棱镜七彩信息科技有限公司	2	2
国网山东省电力公司	2	2
华鲁数智信息技术（北京）有限公司	2	2
南京禾盾信息科技有限公司	2	2
上海贝锐信息科技股份有限公司	1	1

厦门星舟科技有限公司	1	1
北京科技大学	1	1
上海上讯信息技术股份有限公司	1	1
开元华创科技集团	1	1
中国烟草总公司湖北省公司	1	1
武汉非尼克斯软件技术有限公司	1	1
广东蓝爵网络安全技术股份有限公司	1	1
思而听网络科技有限公司	1	1
浙江乾冠信息安全研究院	1	1
北京机沃科技有限公司	1	1
CNCERT 宁夏分中心	30	30
CNCERT 浙江分中心	4	4
CNCERT 河北分中心	2	2
CNCERT 云南分中心	1	1
个人	1812	1812
报送总计	6522	4620

本周漏洞按类型和厂商统计

本周，CNVD 收录了 537 个漏洞。WEB 应用 245 个，应用程序 141 个，网络设备（交换机、路由器等网络端设备）77 个，智能设备（物联网终端设备）28 个，操作系统 21 个，数据库 18 个，安全产品 7 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	245
应用程序	141
网络设备（交换机、路由器等网络端设备）	77

智能设备（物联网终端设备）	28
操作系统	21
数据库	18
安全产品	7

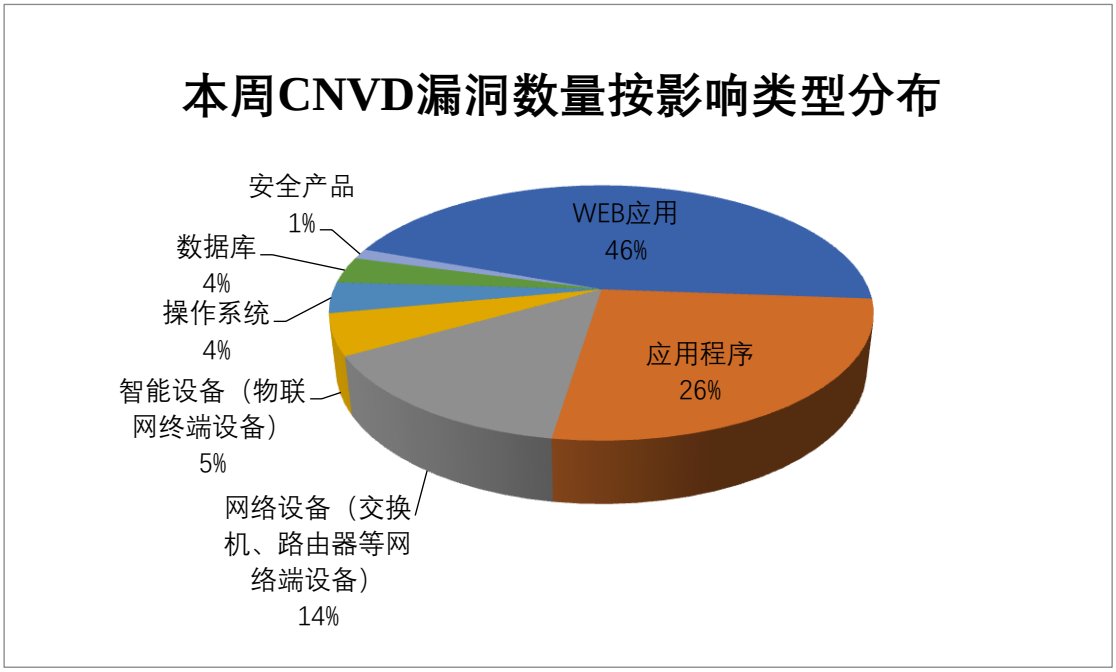

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 WordPress、Foxit、Microsoft 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	35	7%
2	Foxit	21	4%
3	Microsoft	19	3%
4	Adobe	15	2%
5	Tenda	13	2%
6	Six Apart	11	2%
7	TP-LINK	11	2%
8	Pimcore	10	2%
9	GPAC	9	2%
10	其他	393	74%

本周行业漏洞收录情况

本周，CNVD 收录了 56 个电信行业漏洞，9 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，“Tenda AX1806 堆栈溢出漏洞、TP-Link Archer A7 安全绕过漏洞”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/

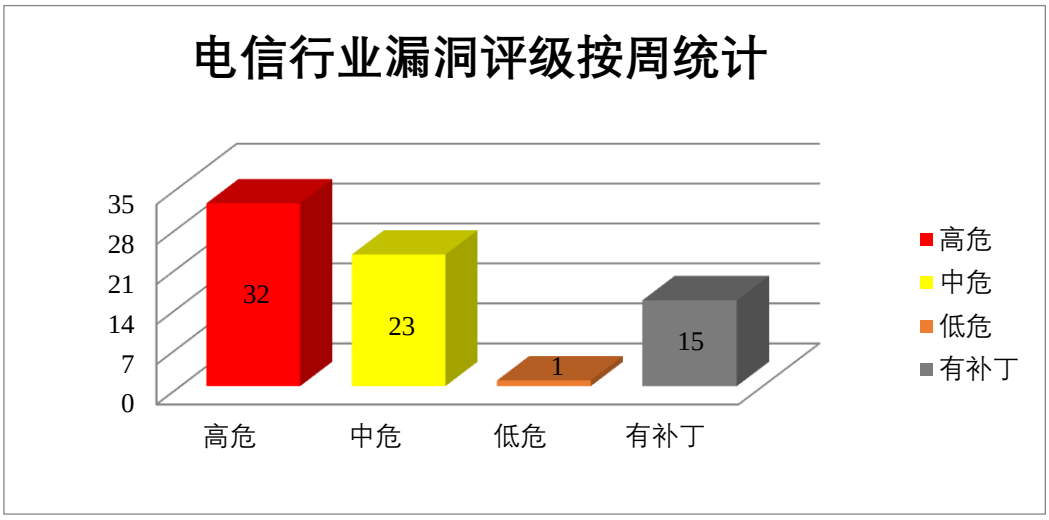

图 3 电信行业漏洞统计

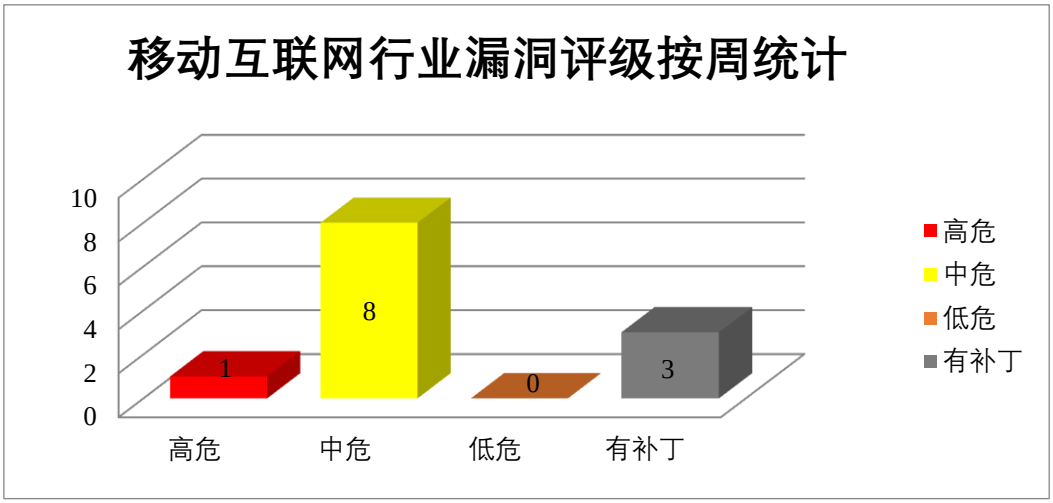

图 4 移动互联网行业漏洞统计

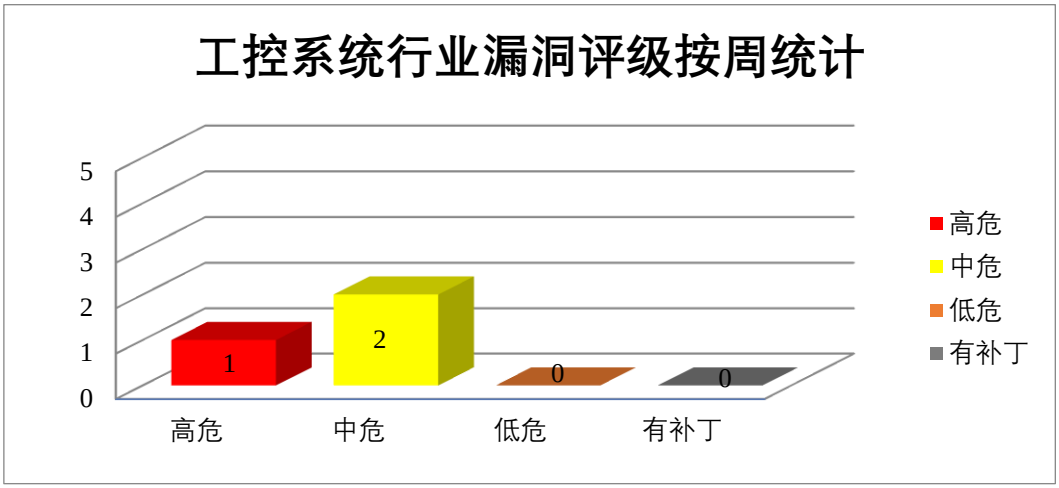

图 5 工控系统行业漏洞统计

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 是中国普联公司的一款无线路由器。Tp-link TL-WR841N 是一款无线路由器。TP-Link TL-WR940N 是一款无线路由器。Tp-link AC1750 是一款无线路由器。TP-Link Archer C1200 是一款无线双频 Gigabit 路由器。TP-Link UE330 USB 是端口 USB 3.0 集线器。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望远镜和光电传感器从设备上的 LED 恢复语音信号，进行“萤火虫”攻击，使应用程序崩溃，在 root 上下文中执行代码等。

CNVD 收录的相关漏洞包括：TP-Link TL-WR886N 栈溢出漏洞（CNVD-2022-21168）、CNVD-2022-21167）、Tp-link TL-WR841N 信任管理问题漏洞、TP-Link TL-WR940N 缓冲区溢出漏洞、TP-Link AC1750 输入验证错误漏洞、TP-Link Archer C1200 跨站脚本漏洞（CNVD-2022-21173）、TP-Link UE330 USB 信息泄露漏洞、TP-Link Archer A7 AC1750 命令注入漏洞。其中，除“TP-Link Archer C1200 跨站脚本漏洞（CNVD-2022-21173）、TP-Link UE330 USB 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-2022-21168

https://www.cnvd.org.cn/flaw/show/CNVD-2022-21167

https://www.cnvd.org.cn/flaw/show/CNVD-2022-21171

https://www.cnvd.org.cn/flaw/show/CNVD-2022-21170

https://www.cnvd.org.cn/flaw/show/CNVD-2022-21169

https://www.cnvd.org.cn/flaw/show/CNVD-2022-21173

https://www.cnvd.org.cn/flaw/show/CNVD-2022-21172

https://www.cnvd.org.cn/flaw/show/CNVD-2022-21176

2、 Adobe 产品安全漏洞

Adobe Photoshop 是美国奥多比（Adobe）公司的一套图片处理软件。该软件主要用于处理图片。Adobe After Effects 是一套视觉效果和动态图形制作软件。Adobe Illustrator 是一套基于向量的图像制作软件。Adobe Commerce 在单一平台上为 B2B 和 B2C 客户构建多渠道商务体验。Adobe Acrobat Reader Dc 是一个 Pdf 阅读工具。用于可靠查看、打印和注释 Pdf 文档。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当前用户上下文中的内存泄漏，在当前用户的上下文中执行任意代码等。

CNVD 收录的相关漏洞包括：Adobe Photoshop 越界读取漏洞（CNVD-2022-22097）、Adobe After Effects 缓冲区溢出漏洞（CNVD-2022-22096、CNVD-2022-22095、CNVD-2022-22099）、Adobe After Effects 越界写入漏洞（CNVD-2022-22094）、Adobe Illustrator 缓冲区溢出漏洞（CNVD-2022-22098）、Adobe Commerce 输入验证错误漏洞（CNVD-2022-22100）、Adobe Acrobat Reader Dc 缓冲区溢出漏洞（CNVD-2022-22658）。其中，除“Adobe Photoshop 越界读取漏洞（CNVD-2022-22097）”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-2022-22097

https://www.cnvd.org.cn/flaw/show/CNVD-2022-22096

https://www.cnvd.org.cn/flaw/show/CNVD-2022-22095

https://www.cnvd.org.cn/flaw/show/CNVD-2022-22094

https://www.cnvd.org.cn/flaw/show/CNVD-2022-22099

https://www.cnvd.org.cn/flaw/show/CNVD-2022-22098

https://www.cnvd.org.cn/flaw/show/CNVD-2022-22100

https://www.cnvd.org.cn/flaw/show/CNVD-2022-22658

3、 Google 产品安全漏洞

Google Android 是美国谷歌（Google）公司的的一套以 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，提升本地权限，造成应用拒绝服务，本地权限提升等。

CNVD 收录的相关漏洞包括：Google Android 权限提升漏洞（CNVD-2022-22949、CNVD-2022-22950、CNVD-2022-22953、CNVD-2022-22952、CNVD-2022-22956、CNVD-2022-22955）、Google Android 信息泄露漏洞、Google Android 拒绝服务漏洞。其中，“Google Android 权限提升漏洞（CNVD-2022-22949、CNVD-2022-22953、CNVD-2022-22956）”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-2022-22949
https://www.cnvd.org.cn/flaw/show/CNVD-2022-22951
https://www.cnvd.org.cn/flaw/show/CNVD-2022-22950
https://www.cnvd.org.cn/flaw/show/CNVD-2022-22953
https://www.cnvd.org.cn/flaw/show/CNVD-2022-22952
https://www.cnvd.org.cn/flaw/show/CNVD-2022-22956
https://www.cnvd.org.cn/flaw/show/CNVD-2022-22955
https://www.cnvd.org.cn/flaw/show/CNVD-2022-22954

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资源管理错误漏洞，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 资源管理错误漏洞（CNVD-2022-22730、CNVD-2022-22729、CNVD-2022-22731、CNVD-2022-22734、CNVD-2022-22736、CNVD-2022-22735、CNVD-2022-22738、CNVD-2022-22740）。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-2022-22730
https://www.cnvd.org.cn/flaw/show/CNVD-2022-22729
https://www.cnvd.org.cn/flaw/show/CNVD-2022-22731
https://www.cnvd.org.cn/flaw/show/CNVD-2022-22734
https://www.cnvd.org.cn/flaw/show/CNVD-2022-22736
https://www.cnvd.org.cn/flaw/show/CNVD-2022-22735
https://www.cnvd.org.cn/flaw/show/CNVD-2022-22738
https://www.cnvd.org.cn/flaw/show/CNVD-2022-22740

5、TOTOLINK A3100R 命令注入漏洞（CNVD-2022-21549）

Totolink A3100R 是中国 Totolink 公司的一系列无线路由器。本周，TOTOLINK A3100R 被披露存在命令注入漏洞。攻击者可利用该漏洞发送特殊的命令数据实现命令注入。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-2022-21549

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-2022-21483	Waitress 环境问题漏洞（CNVD-2022-21483）	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/Pylons/waitress/security/advisories/GHSA-4f7p-27jc-3c36
CNVD-2022-21491	Dell Emc Streaming Data Platform 代码问题漏洞（CNVD-2022-21491）	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.dell.com/support/kbdoc/en-in/000193697/dsa-2021-205-dell-emc-streaming-data-platform-security-update-for-third-party-vulnerabilities
CNVD-2022-21540	gradio 任意代码注入漏洞	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/gradio-app/gradio/security/advisories/GHSA-f8xq-q7px-wg8c
CNVD-2022-21543	Bareos 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://github.com/bareos/bareos/security/advisories/GHSA-4979-8ffj-4q26
CNVD-2022-21542	Linux kernel 拒绝服务漏洞（CNVD-2022-21542）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://bugzilla.redhat.com/show_bug.cgi?id=2059294
CNVD-2022-21547	Zenario CMS 文件上传漏洞（CNVD-2022-21547）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/hieuminhnv/Zenario-CMS-9.0-last-version/issues/2
CNVD-2022-21546	CKEditor4 身份验证漏洞	高	目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载：https://ckeditor.com/cke4/release/CKEditor-4.18.0
CNVD-2022-21548	libvcs 命令注入漏洞	高	目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载：https://github.com/vcs-python/libvcs/pull/306
CNVD-2022-21809	Apache Gobblin 信任管理问题漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://lists.apache.org/thread/3bxf7rbf4zh95r78jtgth6gwhr5fyl2j
CNVD-2022-21812	Maccms 权限提升漏洞	高	目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载：https://github.com/magicblack/macc

			ms10/issues/747

小结：本周，TP-Link 产品被披露存在多个漏洞，攻击者可利用漏洞通过望远镜和光电传感器从设备上的 LED 恢复语音信号，进行“萤火虫”攻击，使应用程序崩溃，在 root 上下文中执行代码等。此外，Adobe、Google、Foxit 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，提升本地权限，造成应用拒绝服务，在当前用户的上下文中执行任意代码。另外，TOTOLINK A3100R 被披露存在命令注入漏洞。攻击者可利用该漏洞发送特殊的命令数据实现命令注入。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、CuppaCMS SQL 注入漏洞（CNVD-2022-22322）

验证描述

CuppaCMS 是一套内容管理系统（CMS）。

CuppaCMS 存在 SQL 注入漏洞，该漏洞源于基于数据库的应用缺少对外部输入 SQL 语句的验证，攻击者可利用该漏洞执行非法 SQL 命令。

验证信息

POC 链接：https://github.com/CuppaCMS/CuppaCMS/issues/13

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2022-22322

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. 戴尔 BIOS 漏洞影响 Inspiron，Vostro，XPS，Alienware 系统

继 Insyde Software 的 InsydeH2O 和 UEFI 最近发现的固件漏洞之后，戴尔 BIOS 中又暴露了五个新的安全漏洞。

参考链接：https://thehackernews.com/2022/03/new-dell-bios-bugs-affect-millions-of.html

2. Sophos 防火墙受到一个身份验证绕过漏洞影响

近期，Sophos 修复了位于 Sophos 防火墙的用户门户和 Webadmin 区域的身份验证绕过漏洞，该漏洞被标记为 CVE-2022-1040。

参考链接：https://www.freebuf.com/news/326433.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