国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2022 年 01 月 10 日-2022 年 01 月 16 日 **2022 年第 2 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 595 个，其中高危漏洞 189 个、中危漏洞 371 个、低危漏洞 35 个。漏洞平均分值为 5.92。本周收录的漏洞中，涉及 0day 漏洞 368 个（占 62%），其中互联网上出现“Bludit 跨站脚本漏洞（CNVD-2022-02493）、Waimai Super Cms 跨站脚本漏洞（CNVD-2022-02739）”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 33637 个，与上周（3412 个）环比增加 886%。

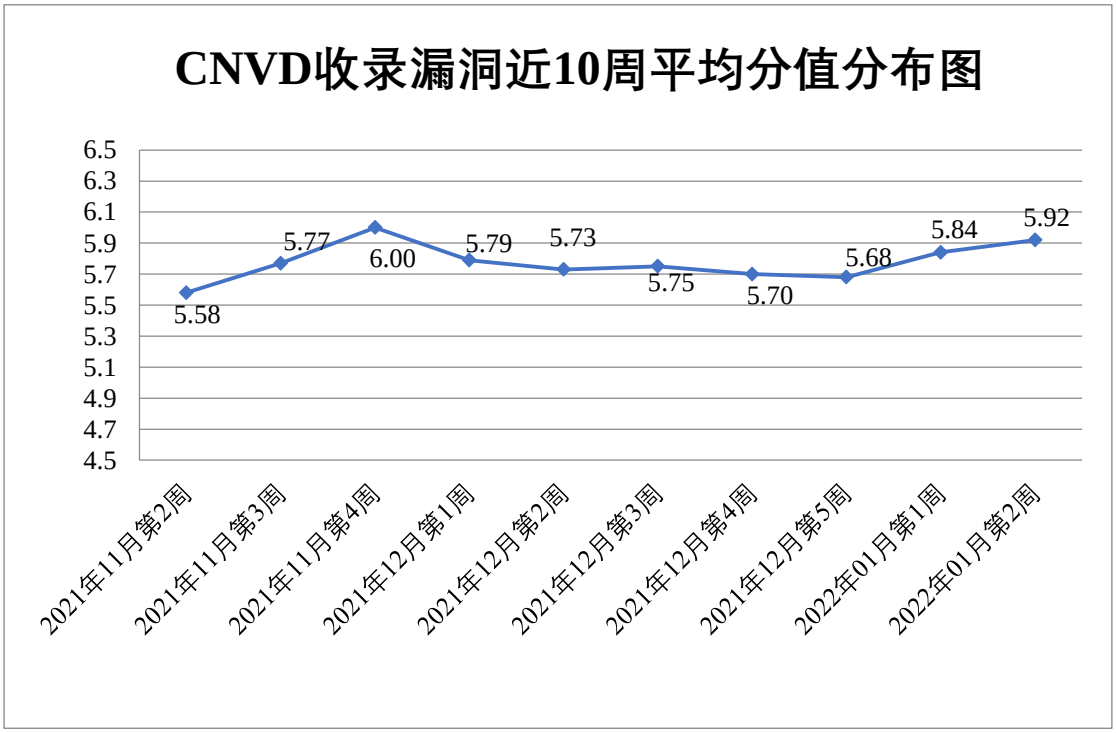

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 37 起，向基础电信企业通报漏洞事件 35 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 1218 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 115 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：

淄博闪灵网络科技有限公司、重庆远秋科技有限公司、浙江宇视科技有限公司、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、新天科技股份有限公司、新开普电子股份有限公司、西安众邦网络科技有限公司、武汉烽火科技集团有限公司、温州互引信息技术有限公司、网件（北京）网络技术有限公司、苏州科达科技股份有限公司、思科系统（中国）网络技术有限公司、深圳市圆梦云科技有限公司、深圳市迅龙软件有限公司、深圳市美科星通信技术有限公司、深圳市麦斯杰网络有限公司、深圳市磊科实业有限公司、深圳市捷视飞通科技股份有限公司、深圳市吉祥腾达科技有限公司、深圳市道尔智控科技股份有限公司、深圳瑞科软件有限公司、深圳警翼智能科技股份有限公司、上海卓越睿新数码科技股份有限公司、上海威派格智慧水务股份有限公司、上海天泰网络技术有限公司、上海华测导航技术股份有限公司、上海恒生聚源数据服务有限公司、上海复翼软件开发有限公司、上海泛微网络科技股份有限公司、上海贝锐信息科技股份有限公司、上海安达通信息安全技术股份有限公司、熵基科技股份有限公司、青岛东胜伟业软件有限公司、青岛东软载波科技股份有限公司、普联技术有限公司、内蒙古浩海商贸有限公司、南京三商电脑软件开发有限公司、南京科远智慧科技集团股份有限公司、南昌卓蓝科技有限公司、迈普通信技术股份有限公司、理光（中国）投资有限公司、朗坤智慧科技股份有限公司、科大讯飞股份有限公司、江西铭软科技有限公司、霍尼韦尔（中国）有限公司、惠普贸易（上海）有限公司、湖南三唐信息科技有限公司、湖南华美信息系统有限公司、湖北华强软件开发有限公司、恒玄科技（上海）股份有限公司、合肥明信软件技术有限公司、杭州易软共创网络科技有限公司、杭州三汇数字信息技术有限公司、海南赞赞网络科技有限公司、桂林崇胜网络科技有限公司、广州齐博网络科技有限公司、广州南方卫星导航仪器有限公司、广东卓锐软件有限公司、广东南方数码科技股份有限公司、富士施乐(中国)有限公司、福建亿同世纪软件科技股份有限公司、飛思達技術（北京）有限公司、畅捷通信息技术股份有限公司、北京中农信达信息技术有限公司、北京中控科技发展有限公司、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、北京山石网科信息技术有限公司、北京良精志诚科技有限责任公司、北京金和网络股份有限公司、北京华宇信息技术有限公司、北京华富远科技术有限公司、北京和信创天科技股份有限公司、北京百卓网络技术有限公司、北京

安易王软件有限公司、奥琦玮信息科技 (北京) 有限公司、若依、WordPress、WDJA、Vmware、Trendnet、taoCMS、seacms、Sapido Technology Inc、Oracle、Glyph & Cog, LLC、BitComet 和 Apache。

本周，CNVD 发布了《Microsoft 发布 2022 年 1 月安全更新》。详情参见 CNVD 网站公告内容 。

https://www.cnvd.org.cn/webinfo/show/7241

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，北京天融信网络安全技术有限公司、安天科技集团股份有限公司、北京神州绿盟科技有限公司、新华三技术有限公司、阿里云计算有限公司等单位报送公开收集的漏洞数量较多。山东泽鹿安全技术有限公司、北京山石网科信息技术有限公司、南京树安信息技术有限公司、重庆都会信息科技、广东蓝爵网络安全技术股份有限公司、河南灵创电子科技有限公司、福建省海峡信息技术有限公司、山东云天安全技术有限公司、河南信安世纪科技有限公司、内蒙古洞明科技有限公司、广州百蕴启辰科技有限公司、广西等保安全测评有限公司、北京水木羽林科技有限公司、国家计算机网络应急技术处理协调中心、贵州多彩宝互联网服务有限公司、思而听网络科技有限公司、杭州美创科技有限公司、天津偕行科技有限公司、快页信息技术有限公司、南京深安科技有限公司、思而听网络科技有限公司、北京威努特技术有限公司、山石网科通信技术股份有限公司、上海视岳计算机科技有限公司、博智安全科技股份有限公司、安徽长泰科技有限公司、深圳昂楷科技有限公司、上海上讯信息技术股份有限公司、杭州海康威视数字技术股份有限公司、中通服和信科技有限公司、广东安创信息科技开发有限公司、浙江木链物联网科技有限公司及其他个人白帽子向 CNVD 提交了 33637 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）、上海交大向 CNVD 共享的白帽子报送的 31439 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）	28794	28794
斗象科技（漏洞盒子）	2209	2209
上海交大	436	436
北京天融信网络安全技术有限公司	242	39
安天科技集团股份有限公司	220	0

北京神州绿盟科技有限公司	196	7
新华三技术有限公司	183	0
阿里云计算有限公司	142	1
恒安嘉新(北京)科技股份公司	120	0
北京华顺信安科技有限公司	107	2
杭州安恒信息技术股份有限公司	71	35
北京启明星辰信息安全技术有限公司	66	2
南京众智维信息科技有限公司	61	61
天津市国瑞数码安全系统股份有限公司	58	0
深信服科技股份有限公司	44	0
北京数字观星科技有限公司	43	0
西安四叶草信息技术有限公司	32	32
厦门服云信息科技有限公司	28	0
中国电信集团系统集成有限责任公司	21	0
京东科技信息技术有限公司	6	6
北京知道创宇信息技术股份有限公司	3	0
北京鸿腾智能科技有限公司	2	2
内蒙古云科数据服务股份有限公司	2	2

北京长亭科技有限公司	2	2
卫士通信息产业股份有限公司	1	1
北京智游网安科技有限公司	1	1
山东泽鹿安全技术有限公司	111	111
北京山石网科信息技术有限公司	58	58
南京树安信息技术有限公司	41	41
重庆都会信息科技	38	38
广东蓝爵网络安全技术股份有限公司	23	23
河南灵创电子科技有限公司	21	21
福建省海峡信息技术有限公司	21	21
山东云天安全技术有限公司	20	20
河南信安世纪科技有限公司	15	15
内蒙古洞明科技有限公司	14	14
广州百蕴启辰科技有限公司	13	13
广西等保安全测评有限公司	8	8
北京水木羽林科技有限公司	7	7
国家计算机网络应急技术处理协调中心	6	6
贵州多彩宝互联网服	5	5

务有限公司		
思而听网络科技有限公司	5	5
杭州美创科技有限公司	4	4
天津偕行科技有限公司	4	4
快页信息技术有限公司	4	4
南京深安科技有限公司	3	3
思而听网络科技有限公司	3	3
北京威努特技术有限公司	2	2
山石网科通信技术股份有限公司	2	2
上海视岳计算机科技有限公司	2	2
博智安全科技股份有限公司	2	2
安徽长泰科技有限公司	1	1
深圳昂楷科技有限公司	1	1
上海上讯信息技术股份有限公司	1	1
杭州海康威视数字技术股份有限公司	1	1
中通服和信科技有限公司	1	1
广东安创信息科技开发有限公司	1	1
浙江木链物联网科技	1	1

有限公司		
中国电信股份有限公司网络安全产品运营中心	59	0
亚信科技（成都）有限公司	26	0
西门子（中国）有限公司	21	0
CNCERT 四川分中心	5	5
CNCERT 贵州分中心	4	4
CNCERT 内蒙古分中心	2	2
CNCERT 云南分中心	1	1
个人	1554	1554
报送总计	35201	33637

本周漏洞按类型和厂商统计

本周，CNVD 收录了 595 个漏洞。WEB 应用 242 个，应用程序 233 个，网络设备（交换机、路由器等网络端设备）83 个，智能设备（物联网终端设备）14 个，操作系统 8 个，数据库 8 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	242
应用程序	233
网络设备（交换机、路由器等网络端设备）	83
智能设备（物联网终端设备）	14
操作系统	8
数据库	8
安全产品	7

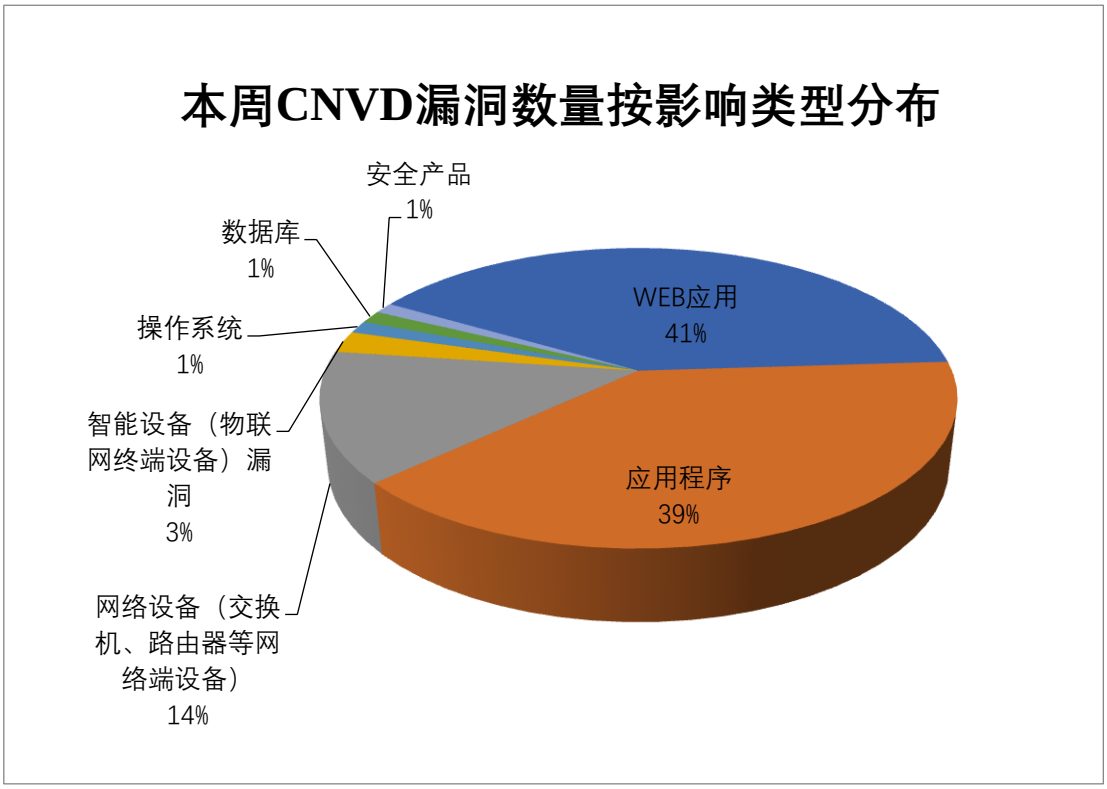

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及淄博闪灵网络科技有限公司、GPAC、Mozilla 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	淄博闪灵网络科技有限公司	32	5%
2	GPAC	29	5%
3	Mozilla	24	4%
4	Apache	21	3%
5	广州中望龙腾软件股份有限公司	20	3%
6	Trendnet	15	3%
7	NETGEAR	15	3%
8	Microsoft	13	2%
9	Oracle	12	2%
10	其他	414	70%

本周行业漏洞收录情况

本周，CNVD 收录了 53 个电信行业漏洞，10 个移动互联网行业漏洞，11 个工控行业漏洞（如下图所示）。其中，“Netgear Nighthawk R6700 授权问题漏洞、Siemens SICAM A8000 硬编码凭证漏洞”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/

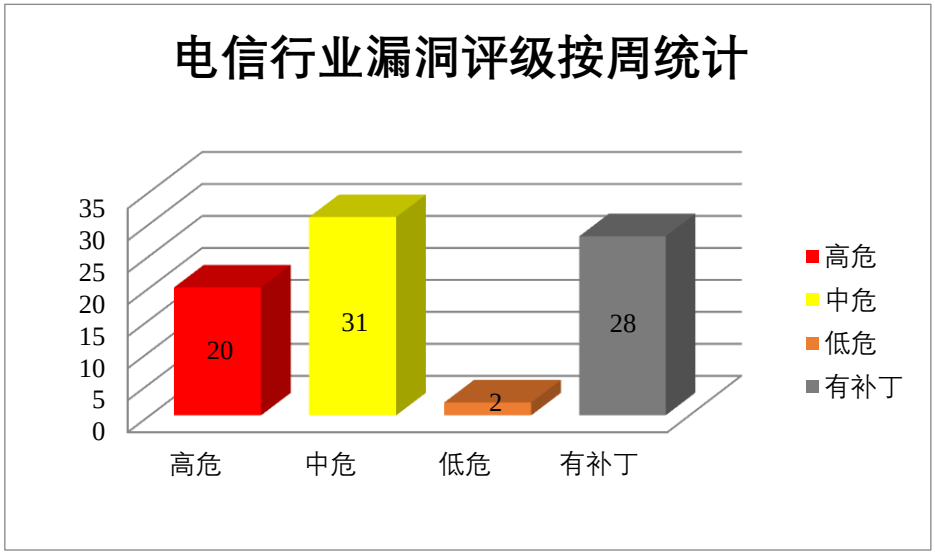

图 3 电信行业漏洞统计

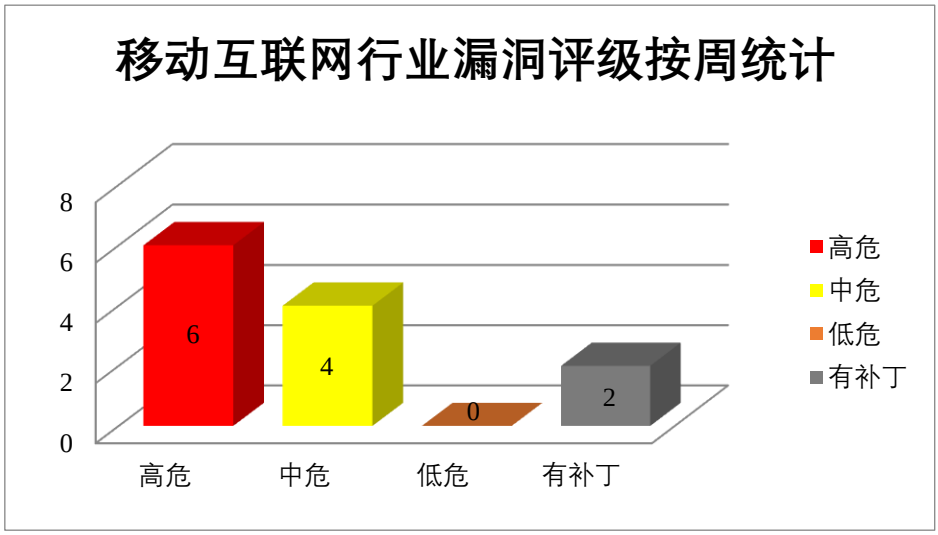

图 4 移动互联网行业漏洞统计

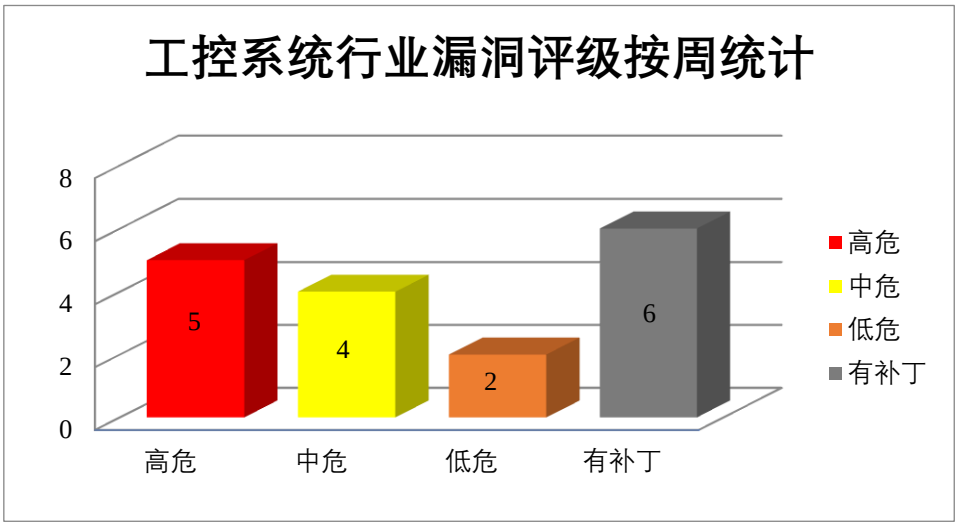

图 5 工控系统行业漏洞统计

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、Oracle 产品安全漏洞

Oracle E-Business Suite 是在原来 Application（ERP）基础上的扩展，包括 ERP（企业资源计划管理）、HR（人力资源管理）、CRM（客户关系管理）等等多种管理软件的集合，是无缝集成的一个管理套件。Oracle Applications Framework 是 Oracle 公司开发的专有框架，用于 Oracle E-Business Suite（Oracle 电子商务套件）中的应用程序开发。Oracle Universal Work Queue 是其中的一个灵活的工作演示和访问工具，可提供工作的集中视图和访问。Oracle Sales Offline 是其中的一款离线销售管理软件。Oracle Incentive Compensation 是其中的一个全球化的浮动薪酬管理软件，可自动设计、管理和分析针对员工和合作伙伴的基于激励机制的报酬计划，从而有效促进企业目标的实现。Oracle Trade Management 是其中的一个支持迭代销售模型的销售应用程序。Oracle Applications Manager (OAM)可让管理员从 HTML 控制台管理 Oracle E-Business Suite 系统。本周，上述产品被披露存在多个漏洞，攻击者可利用该漏洞对 Oracle Trade Management 可访问数据的子集进行未经授权的读取访问，对某些 Oracle Applications Manager 可访问数据的未经授权的更新、插入或删除访问，导致 Oracle 应用程序框架的部分拒绝服务（部分 DOS）等。

CNVD 收录的相关漏洞包括：Oracle E-Business Suite 拒绝服务漏洞（CNVD-2022-02347、CNVD-2022-02348）、Oracle E-Business Suite 未授权访问漏洞（CNVD-2022-02349、CNVD-2022-02351、CNVD-2022-02350、CNVD-2022-02353、CNVD-2022-02352、CNVD-2022-02357）。其中，“Oracle E-Business Suite 未授权访问漏洞（CNVD-2022-02349、CNVD-2022-02357）”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-2022-02347
https://www.cnvd.org.cn/flaw/show/CNVD-2022-02349
https://www.cnvd.org.cn/flaw/show/CNVD-2022-02348
https://www.cnvd.org.cn/flaw/show/CNVD-2022-02351
https://www.cnvd.org.cn/flaw/show/CNVD-2022-02350
https://www.cnvd.org.cn/flaw/show/CNVD-2022-02353
https://www.cnvd.org.cn/flaw/show/CNVD-2022-02352
https://www.cnvd.org.cn/flaw/show/CNVD-2022-02357

2、 Adobe 产品安全漏洞

Adobe Dimension 是美国 Adobe 公司的是一套 2D 和 3D 合成设计工具。Adobe Prelude 是美国奥多比（Adobe）公司的一套视频素材编辑剪辑工具。该产品能够对视频素材进行剪辑、排序和注释等。本周，上述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，导致敏感内存泄露。

CNVD 收录的相关漏洞包括：Adobe Dimension 内存损坏漏洞、Adobe Dimension 越界读取漏洞（CNVD-2022-02631、CNVD-2022-02635、CNVD-2022-02636）、Adobe Dimension 越界写入漏洞（CNVD-2022-02634、CNVD-2022-02633）、Adobe Prelude 内存损坏漏洞（CNVD-2022-02637、CNVD-2022-02638）。其中，“Adobe Dimension 内存损坏漏洞、Adobe Dimension 越界写入漏洞（CNVD-2022-02634、CNVD-2022-02633）、Adobe Prelude 内存损坏漏洞（CNVD-2022-02637、CNVD-2022-02638）”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-2022-02632
https://www.cnvd.org.cn/flaw/show/CNVD-2022-02631
https://www.cnvd.org.cn/flaw/show/CNVD-2022-02635
https://www.cnvd.org.cn/flaw/show/CNVD-2022-02634
https://www.cnvd.org.cn/flaw/show/CNVD-2022-02633
https://www.cnvd.org.cn/flaw/show/CNVD-2022-02636
https://www.cnvd.org.cn/flaw/show/CNVD-2022-02638
https://www.cnvd.org.cn/flaw/show/CNVD-2022-02637

3、 Apache 产品安全漏洞

Apache Kylin 是美国阿帕奇（Apache）基金会的一款开源的分布式分析型数据仓库。该产品主要提供 Hadoop/Spark 之上的 SQL 查询接口及多维分析（OLAP）等功能。Apache Avro 是美国阿帕奇（Apache）基金会的一个数据序列化系统。为 Apache Hadoop

提供数据序列化和数据交换服务。Apache HTTP Server 是美国阿帕奇（Apache）基金会的一款开源网页服务器。该服务器具有快速、可靠且可通过简单的 API 进行扩充的特点。Apache NiFi 是美国阿帕奇（Apache）基金会的一套数据处理和分发系统。该系统主要用于数据路由、转换和系统中介逻辑。本周，上述产品被披露存在多个漏洞，攻击者可利用该漏洞探测服务器内网资源，分配过多资源导致拒绝服务，在 Kylin 服务器进程中执行来自黑客控制的恶意 MySQL 服务器的任意代码。

CNVD 收录的相关漏洞包括：Apache Kylin 输入验证错误漏洞、Apache Kylin 操作系统命令注入漏洞、Apache Kylin 服务端请求伪造漏洞、Apache Kylin 权限许可和访问控制问题漏洞、Apache Avro 资源管理错误漏洞、Apache HTTP Server 目录遍历漏洞、Apache NiFi 操作系统命令注入漏洞、Apache HTTP Server ap_escape_quotes 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-2022-02487
https://www.cnvd.org.cn/flaw/show/CNVD-2022-02489
https://www.cnvd.org.cn/flaw/show/CNVD-2022-02753
https://www.cnvd.org.cn/flaw/show/CNVD-2022-02752
https://www.cnvd.org.cn/flaw/show/CNVD-2022-02754
https://www.cnvd.org.cn/flaw/show/CNVD-2022-03220
https://www.cnvd.org.cn/flaw/show/CNVD-2022-03221
https://www.cnvd.org.cn/flaw/show/CNVD-2022-03225

4、Trendnet 产品安全漏洞

Trendnet AC2600 TEW-827DRU 是一款无线路由器。本周，上述产品被披露存在多个漏洞，攻击者可利用该漏洞强制更改管理员密码，通过 Bittorent web 客户端访问和修改设置和文件，提供格式错误的参数以 root 用户身份注入命令等。

CNVD 收录的相关漏洞包括：Trendnet AC2600 TEW-827DRU 身份验证绕过漏洞、Trendnet AC2600 TEW-827DRU 访问控制错误漏洞、Trendnet AC2600 TEW-827DRU 数据伪造问题漏洞、Trendnet AC2600 TEW-827DRU 命令注入漏洞（CNVD-2022-03198、CNVD-2022-03200）、Trendnet AC2600 TEW-827DRU 信任管理问题漏洞、Trendnet AC2600 TEW-827DRU 拒绝服务漏洞、Trendnet AC2600 TEW-827DRU 加密问题漏洞。除“Trendnet AC2600 TEW-827DRU 访问控制错误漏洞、Trendnet AC2600 TEW-827DRU 数据伪造问题漏洞”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-2022-03191
https://www.cnvd.org.cn/flaw/show/CNVD-2022-03190

https://www.cnvd.org.cn/flaw/show/CNVD-2022-03195

https://www.cnvd.org.cn/flaw/show/CNVD-2022-03198

https://www.cnvd.org.cn/flaw/show/CNVD-2022-03197

https://www.cnvd.org.cn/flaw/show/CNVD-2022-03196

https://www.cnvd.org.cn/flaw/show/CNVD-2022-03200

https://www.cnvd.org.cn/flaw/show/CNVD-2022-03203

5、Google Chrome 越界写入漏洞（CNVD-2022-02736）

Google Chrome 是美国谷歌（Google）公司的一款 Web 浏览器。本周，Google Chrome 被披露存在越界写入漏洞。攻击者可利用该漏洞在系统上执行任意代码。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-2022-02736

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-2022-02644	Netgear RAX43 命令注入漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://www.tenable.com/security/research/tra-2021-55
CNVD-2022-02646	Netgear Genie 权限许可和访问控制问题漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://www.tenable.com/security/research/tra-2021-56
CNVD-2022-02732	Realtek RTL8195AM 缓冲区溢出漏洞	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.amebaiot.com/en/security_bulletin/cve-2021-39306/
CNVD-2022-02737	ZZCMS 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/forget-code/zzcms/issues/1
CNVD-2022-04000	Microsoft Defender for IoT 远程代码执行漏洞（CNVD-2022-04000）	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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42311
CNVD-2022-02747	Siemens COMOS Web 组件跨站脚本漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：

			https://support.industry.siemens.com/cs/ww/en/view/109805632/
CNVD-2022-02746	Siemens COMOS Web 组件路径遍历漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://support.industry.siemens.com/cs/ww/en/view/109805632/
CNVD-2022-02745	Siemens COMOS Web组件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://support.industry.siemens.com/cs/ww/en/view/109805632/
CNVD-2022-02764	Fortinet FortiWLM SQL注入漏洞（CNVD-2022-02764）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.fortiguard.com/psirt/FG-IR-21-129
CNVD-2022-02765	Amios Emuse-eServices/eNvoice 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://www.eservicestech.com/
CNVD-2022-03186	Atlassian Jira 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://jira.atlassian.com/browse/JRASERVER-73067
CNVD-2022-03206	IBM AIX 权限许可和访问控制问题漏洞（CNVD-2022-03206）	高	厂商已发布了漏洞修复程序，请及时关注更新：http://aix.software.ibm.com/aix/efixes/security/mount_advisory.asc
CNVD-2022-03210	WordPress 跨站脚本漏洞（CNVD-2022-03210）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/WordPress/wordpress-develop/security/advisories/GHSA-699q-3hj9-889w
CNVD-2022-03901	ToTolink Ex200 命令注入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/doudoudedi/ToTolink_EX200_Cmmand_Execute/blob/main/ToTolink%20EX200%20Comand%20Injection2.md
CNVD-2022-03910	Bundler 代码注入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/rubygems/rubygems/security/advisories/GHSA-fj7f-vq84-fh43
CNVD-2022-03917	ZOHO ManageEngine Remote Access Plus 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：https://medium.com/nestedif/vulnera

			bility-disclosure-improper-acl-unauthorized-password-reset-zoho-r-a-p-62efcdceb7a6
CNVD-2022-03956	radare2 缓冲区溢出漏洞（CNVD-2022-03956）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://huntr.dev/bounties/727d8600-88bc-4dde-8dea-ee3d192600e5
CNVD-2022-03955	IBM VIOS 操作系统命令注入漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：http://aix.software.ibm.com/aix/efixes/security/lscore_advisory.asc
CNVD-2022-03999	Microsoft Defender for IoT 远程代码执行漏洞（CNVD-2022-03999）	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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42313
CNVD-2022-03998	Microsoft Defender for IoT 远程代码执行漏洞（CNVD-2022-03998）	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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42315

小结：本周，Oracle 产品被披露存在多个漏洞，攻击者可利用该漏洞对 Oracle Trade Management 可访问数据的子集进行未经授权的读取访问，对某些 Oracle Applications Manager 可访问数据的未经授权的更新、插入或删除访问，导致 Oracle 应用程序框架的部分拒绝服务（部分 DOS）等。此外，Adobe、Apache、Trendnet 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，导致敏感内存泄露，执行任意代码，探测服务器内网资源，分配过多资源导致拒绝服务等。另外，Google Chrome 被披露存在越界写入漏洞。攻击者可利用该漏洞在系统上执行任意代码。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、Waimai Super Cms 跨站脚本漏洞（CNVD-2022-02739）

验证描述

Waimai Super Cms 是一套外卖订餐系统。

waimai Super Cms 中存在跨站脚本漏洞，该漏洞源于产品的/admin.php?&m=Public&a=login 链接未能正确处理输入数据。攻击者可通过该漏洞导致客户端代码执行。

验证信息

POC 链接：https://github.com/caokang/waimai/issues/16

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2022-02739

信息提供者

北京天融信网络安全技术有限公司

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. Linux 恶意软件在 2021 年增长 35%

2021 年，针对 Linux 设备的恶意软件感染数量增加了 35%，最常见的是通过物联网设备进行 DDoS（分布式拒绝服务）攻击。

参考链接：https://www.bleepingcomputer.com/news/security/linux-malware-sees-35-percent-growth-during-2021/?__cf_chl_f_tk=o_c5eY2D4TwNJLz3sCniqv_4IGfb0bI8FIcTRewYAR4-1642396814-0-gaNycGzNDCU

2. Android 用户现可禁用 2G 来阻止 Stingray 攻击

谷歌终于在 Android 上推出了一个选项，允许用户禁用 2G 连接，否则会带来许多蜂窝站点模拟器利用的隐私和安全问题。

参考链接：https://www.bleepingcomputer.com/news/security/android-users-can-now-disable-2g-to-block-stingray-attacks/

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