国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2023 年 01 月 09 日-2023 年 01 月 15 日 **2023 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 231 个，其中高危漏洞 126 个、中危漏洞 101 个、低危漏洞 4 个。漏洞平均分值为 6.92。本周收录的漏洞中，涉及 0day 漏洞 184 个（占 80%），其中互联网上出现“HTMLMinifier 拒绝服务漏洞、Open5GS ngap-handler.c 拒绝服务漏洞”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 4084 个，与上周（4085 个）环比减少 0.02%。

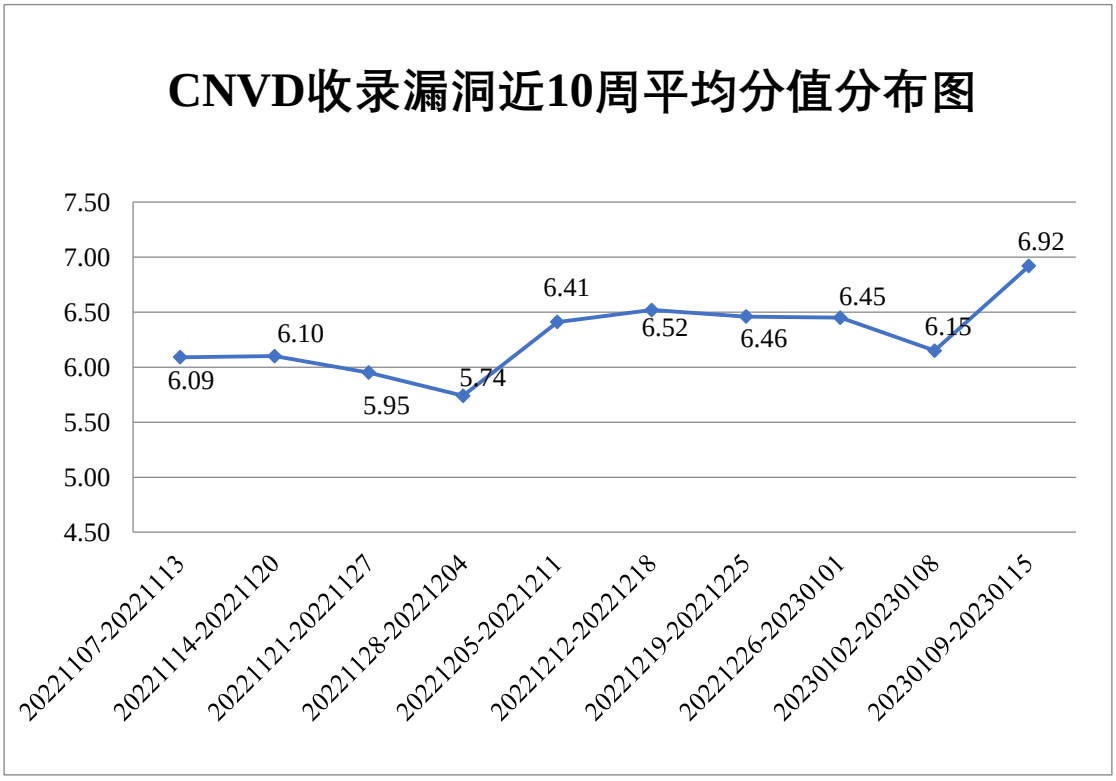

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 39 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 685 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 229 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 88 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：

珠海华发新科技投资控股有限公司、珠海海露智能物联有限公司、珠海国津软件科技有限公司、重庆中联信息产业有限责任公司、众勤通信设备贸易（上海）有限公司、政和科技股份有限公司、浙江宇视科技有限公司、浙江深大智能集团、浙江兰德纵横网络技术股份有限公司、浙江和达科技股份有限公司、浙江东经科技股份有限公司、浙江大华技术股份有限公司、用友网络科技股份有限公司、易事特集团股份有限公司、新都（青岛）办公设备有限公司、夏普商贸（中国）有限公司、武汉天地伟业科技有限公司、武汉金同方科技有限公司、网神信息技术（北京）股份有限公司、天维尔信息科技股份有限公司、天津天堰科技股份有限公司、天地（常州）自动化股份有限公司、速达软件技术（广州）有限公司、苏州科达科技股份有限公司、四平市九州易通科技有限公司、四川健力生科技有限公司、神州数码控股有限公司、深圳智慧光迅信息技术有限公司、深圳维盟科技股份有限公司、深圳市腾讯计算机系统有限公司、深圳市他知电子商务有限公司、深圳市联软科技股份有限公司、深圳市捷顺科技实业股份有限公司、深圳市捷道智控实业有限公司、深圳市必联电子有限公司、深圳邦健生物医疗设备股份有限公司、上海卓卓网络科技有限公司、上海英立视数字科技有限公司、上海索昂软件科技有限公司、上海商派网络科技有限公司、上海商鼎软件科技有限公司、上海泛微网络科技股份有限公司、上海宝信软件股份有限公司、上海阿法迪智能数字科技股份有限公司、商派软件有限公司、山西复盛公药业集团有限公司、山西复盛公健康药业有限公司、厦门网中网软件有限公司、厦门四信通信科技有限公司、瑞斯康达科技发展股份有限公司、日冲商业（北京）有限公司、青岛中域教育信息咨询有限公司、青岛易软天创网络科技有限公司、青岛海威茨仪表有限公司、青岛东软载波科技股份有限公司、宁波和利时信息安全研究院、浪潮电子信息产业股份有限公司、廊坊市极致网络科技有限公司、嘉兴慕梵传媒科技有限公司、华帝股份有限公司、湖南智擎科技有限公司、湖南省众达数蔚信息技术有限公司、湖南强智科技发展有限公司、湖北京山轻工机械股份有限公司、杭州先锋电子技术股份有限公司、杭州乐湾科技有限公司、杭州荷花软件有限公司、杭州安恒信息技术股份有限公司、广州齐博网络科技有限公司、广州和晖科技有限公司、广东飞企互联科技股份有限公司、东方网力科技股份有限公司、东方电子股份有限公司、成都任我行软件股份有限公司、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、北京中控智慧科技发展有限公司、北京致远互联软件股份有限公司、北京星网锐捷网络技术有限公司、北京新起点盛和教育科技有限公司、北京新发地掌鲜网络科技服务有限公司、北京网康科技有限公司、北京时空智友科技有限公司、北京神州数码云科信息技术有限公司、北京欧倍尔软件技术开发有限公司、北京美特软件技术有限公司、北京六方云信息技术有限公司、北京快猫星云科技有限公司、北京九思协同软件有限公司、北京金和网络股份有限公司、北京健易保科技有限公司、北京宏景世纪软件股份有限公司、北京和利时集团、北京传影科技有限公司、北京百卓网络技术有限公司、北京八十一星网络科技有限公司和安徽青柿信息科技有限公司。

本周，CNVD 发布了《Microsoft 发布 2023 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/8476

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、深信服科技股份有限公司、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等单位报送公开收集的漏洞数量较多。上海齐同信息科技有限公司、博智安全科技股份有限公司、赛尔网络有限公司、快页信息技术有限公司、浙江木链物联网科技有限公司、奇安星城网络安全运营服务（长沙）有限公司、河南东方云盾信息技术有限公司、杭州默安科技有限公司、苏州棱镜七彩信息科技有限公司、杭州美创科技有限公司、北京山石网科信息技术有限公司、北京网猿科技有限公司、山东新潮信息技术有限公司、重庆易阅科技有限公司、安徽锋刃信息科技有限公司、内蒙古洞明科技有限公司、广东唯顶信息科技股份有限公司、长春嘉诚信息技术股份有限公司、北京升鑫网络科技有限公司、内蒙古信元网络安全技术股份有限公司、山东九域信息技术有限公司、山东云天安全技术有限公司、江苏保旺达软件技术有限公司、平安银河实验室、重庆都会信息科技有限公司、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、北京六方云信息技术有限公司、广西等保安全测评有限公司、北京宇天恒瑞科技发展有限公司、北京机沃科技有限公司、河南灵创电子科技有限公司、中通服创发科技有限责任公司、任子行网络技术股份有限公司及其他个人白帽子向 CNVD 提交了 4084 个以事件型漏洞为主的原创漏洞，其中包括奇安信网神（补天平台）、上海交大和斗象科技（漏洞盒子）向 CNVD 共享的白帽子报送的 1950 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）	1100	1100

上海交大	539	539
新华三技术有限公司	460	0
深信服科技股份有限公司	383	0
斗象科技（漏洞盒子）	311	311
安天科技集团股份有限公司	297	0
北京数字观星科技有限公司	224	0
北京启明星辰信息安全技术有限公司	196	24
西安四叶草信息技术有限公司	181	181
阿里云计算有限公司	149	0
杭州安恒信息技术股份有限公司	118	62
北京天融信网络安全技术有限公司	101	0
恒安嘉新（北京）科技股份公司	97	0
远江盛邦（北京）网络安全科技股份有限公司	73	73
南京众智维信息科技有限公司	56	56
中国电信集团系统集成有限责任公司	30	0
京东科技信息技术有限公司	17	6
杭州迪普科技股份有限公司	14	0
北京知道创宇信息技术股份有限公司	5	0
北京长亭科技有限公司	2	2

上海齐同信息科技有限公司	154	154
北京华顺信安信息技术有限公司	90	0
博智安全科技股份有限公司	42	42
赛尔网络有限公司	30	30
快页信息技术有限公司	26	26
浙江木链物联网科技有限公司	24	24
奇安星城网络安全运营服务（长沙）有限公司	19	19
河南东方云盾信息技术有限公司	17	17
杭州默安科技有限公司	15	15
苏州棱镜七彩信息科技有限公司	14	14
杭州美创科技有限公司	11	11
北京山石网科信息技术有限公司	10	10
北京网猿科技有限公司	9	9
山东新潮信息技术有限公司	9	9
重庆易阅科技有限公司	9	9
安徽锋刃信息科技有限公司	9	9
西门子（中国）有限公司	9	0
内蒙古洞明科技有限	8	8

公司		
广东唯顶信息科技股份有限公司	6	6
长春嘉诚信息技术股份有限公司	5	5
北京升鑫网络科技有限公司	5	5
内蒙古信元网络安全技术股份有限公司	4	4
山东九域信息技术有限公司	4	4
山东云天安全技术有限公司	3	3
江苏保旺达软件技术有限公司	3	3
平安银河实验室	3	3
重庆都会信息科技有限公司	2	2
北京华云安信息技术有限公司	2	2
杭州海康威视数字技术股份有限公司	2	2
北京六方云信息技术有限公司	1	1
广西等保安全测评有限公司	1	1
北京宇天恒瑞科技发展有限公司	1	1
北京机沃科技有限公司	1	1
河南灵创电子科技有限公司	1	1
中通服创发科技有限责任公司	1	1
任子行网络技术股份	1	1

有限公司		
CNCERT 浙江分中心	7	7
CNCERT 贵州分中心	4	4
个人	1267	1267
报送总计	6182	4084

本周漏洞按类型和厂商统计

本周，CNVD 收录了 231 个漏洞。WEB 应用 90 个，应用程序 69 个，网络设备（交换机、路由器等网络端设备）57 个，智能设备（物联网终端设备）8 个，操作系统 4 个，安全产品 3 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	90
应用程序	69
网络设备（交换机、路由器等网络端设备）	57
智能设备（物联网终端设备）	8
操作系统	4
安全产品	3

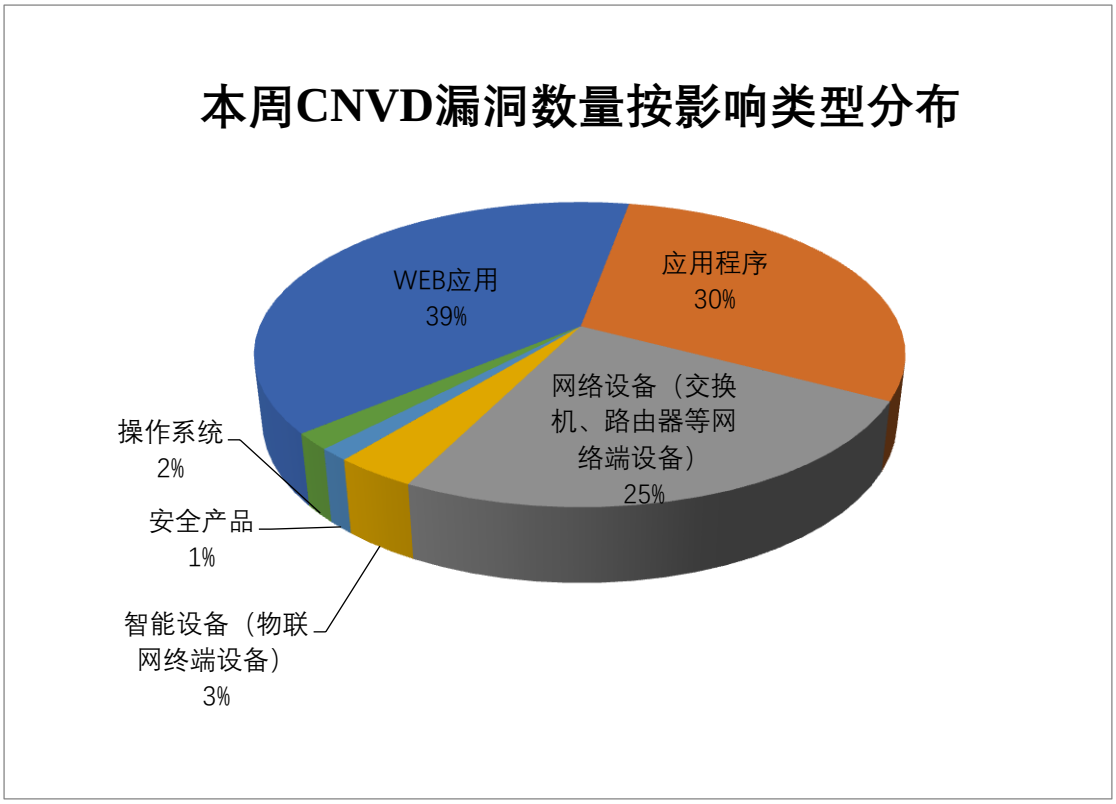

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Tenda、阿里巴巴（中国）网络技术有限公司、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	Tenda	21	9%
2	阿里巴巴（中国）网络技术有限公司	11	5%
3	Microsoft	11	5%
4	Fortinet	10	4%
5	OpenImageIO	10	4%
6	Apache	9	4%
7	SIEMENS	9	4%
8	浙江淘宝网络有限公司	9	4%
9	新华三技术有限公司	8	3%
10	其他	133	58%

本周行业漏洞收录情况

本周，CNVD 收录了 33 个电信行业漏洞，4 个移动互联网行业漏洞，5 个工控行业漏洞（如下图所示）。其中，“Siemens Automation License Manager 路径遍历漏洞、Siemens Automation License Manager 文件名或路径的外部控制漏洞”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/

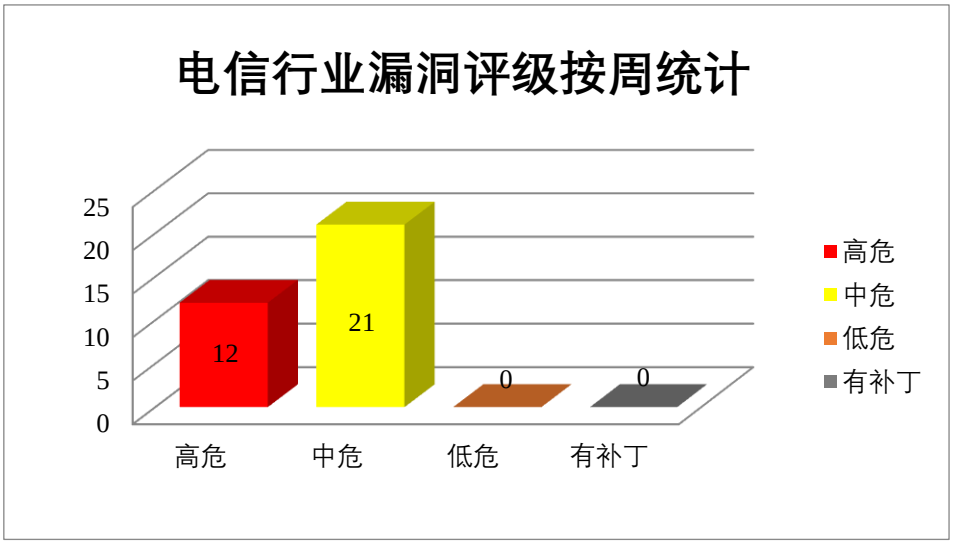

图 3 电信行业漏洞统计

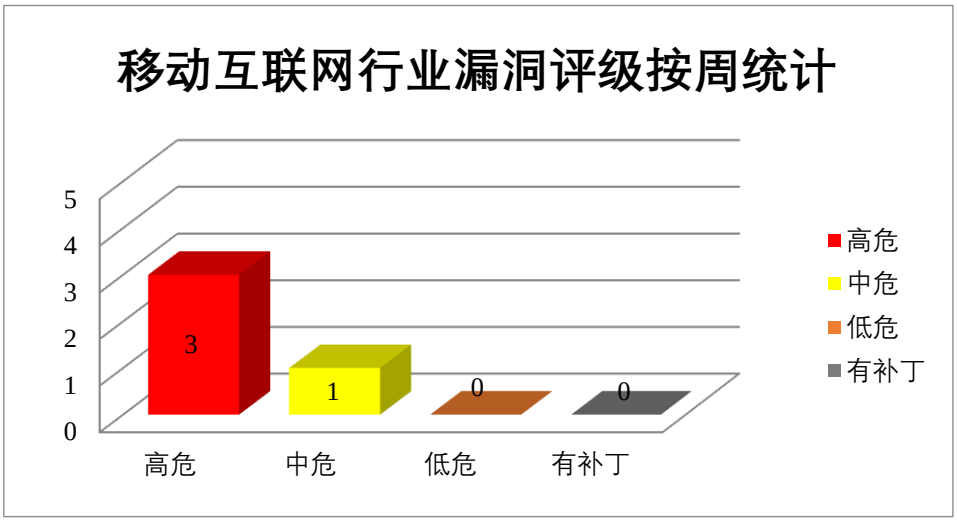

图 4 移动互联网行业漏洞统计

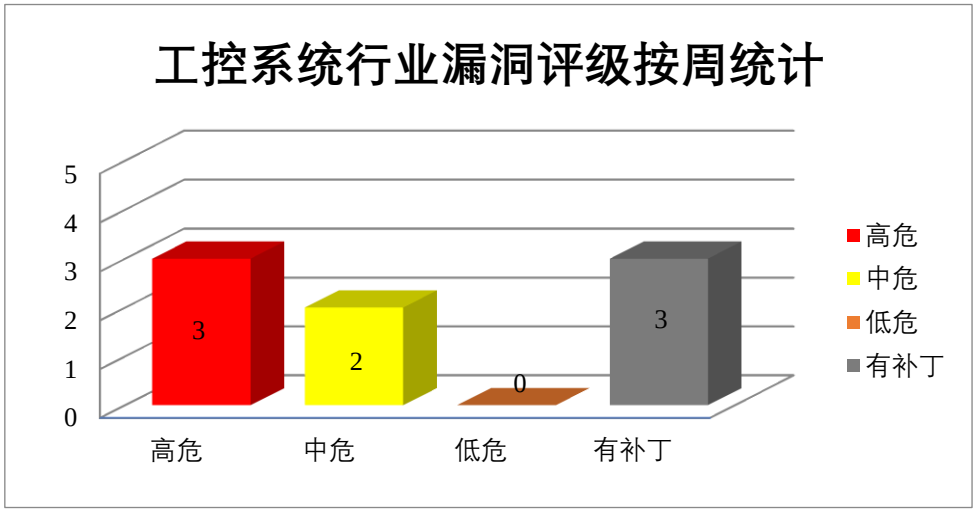

图 5 工控系统行业漏洞统计

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、 Microsoft 产品安全漏洞

Microsoft Word 是美国微软（Microsoft）公司的一套 Office 套件中的文字处理软件。Raw Image Extension 是美国微软（Microsoft）公司的一个用于操作 Raw 格式文件的软件。Microsoft Media Foundation 是适用于 Windows 的下一代多媒体平台。Microsoft Windows Hyper-V 是美国微软（Microsoft）公司的一款可提供硬件虚拟化的工具。Microsoft Excel 是美国微软（Microsoft）公司的一款 Office 套件中的电子表格处理软件。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 Error Reporting（WER）是其中的一个错误报告组件。Power Shell 是美国微软（Microsoft）公司开发的任务自动化和组态管理框架，由.NET Frame

work 和.NET Core 构建的命令列介面壳层相关手稿语言组成。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，提升权限，在系统上执行任意代码等。

CNVD 收录的相关漏洞包括：Microsoft PowerShell 远程代码执行漏洞、Microsoft Word 安全绕过漏洞、Microsoft Raw Image Extension 远程代码执行漏洞（CNVD-2023-02188）、Microsoft Media Foundation 信息泄露漏洞、Microsoft Windows Hyper-V 远程代码执行漏洞（CNVD-2023-02190、CNVD-2023-02191）、Microsoft Excel 远程代码执行漏洞（CNVD-2023-02194）、Microsoft Windows Error Reporting 权限提升漏洞（CNVD-2023-02195）。其中，“Microsoft PowerShell 远程代码执行漏洞、Microsoft Windows Error Reporting 权限提升漏洞（CNVD-2023-02195）”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-2023-01829
https://www.cnvd.org.cn/flaw/show/CNVD-2023-02187
https://www.cnvd.org.cn/flaw/show/CNVD-2023-02188
https://www.cnvd.org.cn/flaw/show/CNVD-2023-02189
https://www.cnvd.org.cn/flaw/show/CNVD-2023-02190
https://www.cnvd.org.cn/flaw/show/CNVD-2023-02191
https://www.cnvd.org.cn/flaw/show/CNVD-2023-02194
https://www.cnvd.org.cn/flaw/show/CNVD-2023-02195

2、Fortinet 产品安全漏洞

Fortinet FortiADC 是美国飞塔（Fortinet）公司的一款应用交付控制器。Fortinet FortiPortal 是美国飞塔（Fortinet）公司的 FortiGate、FortiWiFi 和 FortiAP 产品线的高级、功能丰富的托管安全分析和管理支持工具，可作为虚拟机供 MSP 使用。Fortinet FortiSOAR 是美国飞塔（Fortinet）公司的一种安全编排、自动化和响应（SOAR）解决方案。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，执行客户端代码等。

CNVD 收录的相关漏洞包括：Fortinet FortiADC 操作系统命令注入漏洞、Fortinet FortiPortal 跨站脚本漏洞、Fortinet FortiADC SQL 注入漏洞（CNVD-2023-02484）、Fortinet FortiADC 输入验证错误漏洞、Fortinet FortiSOAR 权限管理错误漏洞、Fortinet FortiSOAR 访问控制错误漏洞（CNVD-2023-02490）、Fortinet FortiADC 跨站脚本漏洞（CNVD-2023-02489）、Fortinet FortiADC 授权问题漏洞。其中，“Fortinet FortiADC 操作系统命令注入漏洞、Fortinet FortiADC SQL 注入漏洞（CNVD-2023-02484）”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-2023-02481

https://www.cnvd.org.cn/flaw/show/CNVD-2023-02480

https://www.cnvd.org.cn/flaw/show/CNVD-2023-02484

https://www.cnvd.org.cn/flaw/show/CNVD-2023-02485

https://www.cnvd.org.cn/flaw/show/CNVD-2023-02488

https://www.cnvd.org.cn/flaw/show/CNVD-2023-02490

https://www.cnvd.org.cn/flaw/show/CNVD-2023-02489

https://www.cnvd.org.cn/flaw/show/CNVD-2023-02491

3、 Apache 产品安全漏洞

Apache Geode 是美国阿帕奇（Apache）基金会的一套应用于分布式云架构中提供对数据密集型应用程序实时和一致访问数据的管理平台。Apache Zeppelin 是美国阿帕奇（Apache）基金会的一款基于 Web 的开源笔记本应用程序。该程序支持交互式数据分析和协作文档。Apache Traffic Server（ATS）是美国阿帕奇（Apache）基金会的一套可扩展的 HTTP 代理和缓存服务器。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 Struts 是美国阿帕奇（Apache）基金会的一个用于开发 Java EE 网络应用程序的开放源代码网页应用程序架构。Apache Geode 是美国阿帕奇（Apache）基金会的一套应用于分布式云架构中提供对数据密集型应用程序实时和一致访问数据的管理平台。Apache Sling Commons Messaging Mail 是美国 Apache 基金会的一款开源消息传递邮件服务。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞删除任意文件，导致服务器崩溃，远程代码执行等。

CNVD 收录的相关漏洞包括：Apache Geode 远程代码执行漏洞（CNVD-2022-83594、CNVD-2022-83596、CNVD-2022-83595）、Apache Zeppelin 输入验证错误漏洞、Apache Traffic Server 异常情况处理错误漏洞、Apache Kylin 命令注入漏洞、Apache Struts 远程代码执行漏洞（CNVD-2023-02478）、Apache Sling Commons Messaging Mail 信任管理问题漏洞。其中，除“Apache Geode 远程代码执行漏洞（CNVD-2022-83594）、Apache Zeppelin 输入验证错误漏洞、Apache Sling Commons Messaging Mail 信任管理问题漏洞”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-2022-83594

https://www.cnvd.org.cn/flaw/show/CNVD-2023-02477

https://www.cnvd.org.cn/flaw/show/CNVD-2023-02476

https://www.cnvd.org.cn/flaw/show/CNVD-2023-02475

https://www.cnvd.org.cn/flaw/show/CNVD-2023-02478

https://www.cnvd.org.cn/flaw/show/CNVD-2022-83596

https://www.cnvd.org.cn/flaw/show/CNVD-2022-83595

https://www.cnvd.org.cn/flaw/show/CNVD-2023-02479

4、Siemens 产品安全漏洞

Solid Edge 是一个软件工具组合，用于处理各种产品开发过程：3D 设计、仿真、制造和设计管理。Automation License Manager（ALM）集中管理各种西门子软件产品的许可证密钥。需要许可证密钥的软件产品会自动向 ALM 报告此要求。当 ALM 找到此软件的有效许可证密钥时，可以根据最终用户许可协议使用该软件。Mendix SAML module 使用 SAML 对云应用程序中的用户进行身份验证。该模块可以与任何支持 SAML2.0 或 Shibboleth 的身份提供程序通信。JT Open Toolkit 是为支持 JT 的软件开发人员提供的应用程序编程接口（API）。JT 是由西门子数字工业软件开发的公开发布的数据格式，广泛用于通信、可视化、数字模型和各种其他目的。Solid Edge 是一个软件工具组合，用于处理各种产品开发过程。SINEC INS（基础设施网络服务）是一个基于 web 的应用程序，将各种网络服务结合在一个工具中。这简化了与工业网络相关的所有网络服务的安装和管理。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诱骗用户访问恶意链接来提取敏感信息，对指定根文件夹之外的文件执行文件操作，在当前进程的上下文中执行代码等。

CNVD 收录的相关漏洞包括：Siemens Solid Edge 文件解析漏洞、Siemens Automation License Manager 路径遍历漏洞、Siemens Mendix SAML Module 跨站脚本漏洞（CNVD-2023-02702）、Siemens JT Open，JT Utilities and Solid Edge 内存损坏漏洞、Siemens SINEC INS 路径遍历漏洞（CNVD-2023-02708、CNVD-2023-02707）、Siemens SINEC INS 命令注入漏洞、Siemens Automation License Manager 文件名或路径的外部控制漏洞。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-2023-02700

https://www.cnvd.org.cn/flaw/show/CNVD-2023-02704

https://www.cnvd.org.cn/flaw/show/CNVD-2023-02702

https://www.cnvd.org.cn/flaw/show/CNVD-2023-02701

https://www.cnvd.org.cn/flaw/show/CNVD-2023-02708

https://www.cnvd.org.cn/flaw/show/CNVD-2023-02707

https://www.cnvd.org.cn/flaw/show/CNVD-2023-02706

https://www.cnvd.org.cn/flaw/show/CNVD-2023-02705

5、Tenda A15 wrlEn 参数堆栈溢出漏洞

Tenda A15 是中国腾达（Tenda）公司的一款 WiFi 扩展器。本周，Tenda A15 被披露存在堆栈溢出漏洞。该漏洞是由于/goform/WifiBasicSet 进行的不正确边界检查造成的。通过使用 wrlEn 参数发送过长的字符串，远程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-2023-02197

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-2023-01829	Microsoft PowerShell 远程代码执行漏洞	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://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-41076
CNVD-2023-02195	Microsoft Windows Error Reporting 权限提升漏洞（CNVD-2023-02195）	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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-24090
CNVD-2023-02269	WordPress WPQA Builder 跨站请求伪造漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://wpscan.com/vulnerability/03b2c6e6-b86e-4143-a84a-7a99060c4848
CNVD-2023-02270	ZOHO ManageEngine ADManager Plus 存在命令执行漏洞	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.manageengine.com/products/ad-manager/admanager-kb/cve-2022-42904.html
CNVD-2023-02271	WBCE CMS 访问控制错误漏洞	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/wbce/wbce_cms/commit/d394ba39a7bfeb31eda797b6195fd90ef74b2e75
CNVD-2023-02478	Apache Struts 远程代码执行漏洞（CNVD-2023-02478）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://struts.apache.org/download.cgi#struts-ga
CNVD-2023-02484	Fortinet FortiADC SQL 注入漏洞（CNVD-2023-02484）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://fortiguard.com/psirt/FG-IR-21-170
CNVD-2023-02704	Siemens Automation License Manager 路径遍历漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://cert-portal.siemens.com/productcert/html/ssa-476715.html

CNVD-2023-02706	Siemens SINEC INS 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://cert-portal.siemens.com/productcert/html/ssa-332410.html
CNVD-2023-02709	禅道项目管理系统远程命令执行漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.zentao.net

小结：本周，Microsoft 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，提升权限，在系统上执行任意代码等。此外，Fortinet、Apache、Siemens 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，删除任意文件，导致服务器崩溃，执行客户端代码等。另外，Tenda A15 被披露存在堆栈溢出漏洞，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、HTMLMinifier 拒绝服务漏洞

验证描述

HTMLMinifier 是一个基于 Javascript 的 HTML 压缩器/迷你器。

HTMLMinifier 4.0.0 版本存在拒绝服务漏洞，该漏洞源于程序使用不当的正则表达式，攻击者可利用该漏洞通过发送特制的正则表达式输入，造成拒绝服务。

验证信息

POC 链接：https://github.com/kangax/html-minifier/blob/51ce10f4daedb1de483ffbcccecc41be1c873da2/src/htmlminifier.js#L294

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2023-02268

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. 多个项目使用的 jsonwebtoken 库中发现安全漏洞

开源 jsonwebtoken (JWT) 库中披露了一个安全漏洞，如果被成功利用，可能会导致在目标服务器上远程执行代码。

参考链接：https://thehackernews.com/2023/01/critical-security-flaw-found-in.html

2. 瑞士军队安全通信软件曝出安全漏洞

近日，苏黎世联邦理工学院研究人员在安全审计中发现瑞士军队使用的安全通信软件 Threema 存在安全漏洞，并且已经存在很长时间。该大学的应用密码学小组本周发布了研究论文，详细介绍了 Threema 自主开发的密码协议中的七个安全漏洞。利用这些漏洞，不法分子将能克隆帐户并读取用户消息，窃取私钥和联系人，甚至出于勒索目的炮制有害资料。

参考链接：https://breakingthe3ma.app/files/Threema-PST22.pdf

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