国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2024 年 04 月 22 日-2024 年 04 月 28 日 **2024 年第 17 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 623 个，其中高危漏洞 240 个、中危漏洞 361 个、低危漏洞 22 个。漏洞平均分值为 6.18。本周收录的漏洞中，涉及 0day 漏洞 466 个（占 75%），其中互联网上出现“Online Courseware editt.php 文件跨站脚本漏洞、Online Book System Product.php 文件 SQL 注入漏洞”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漏洞总数 7766 个，与上周（19674 个）环比减少 61%。

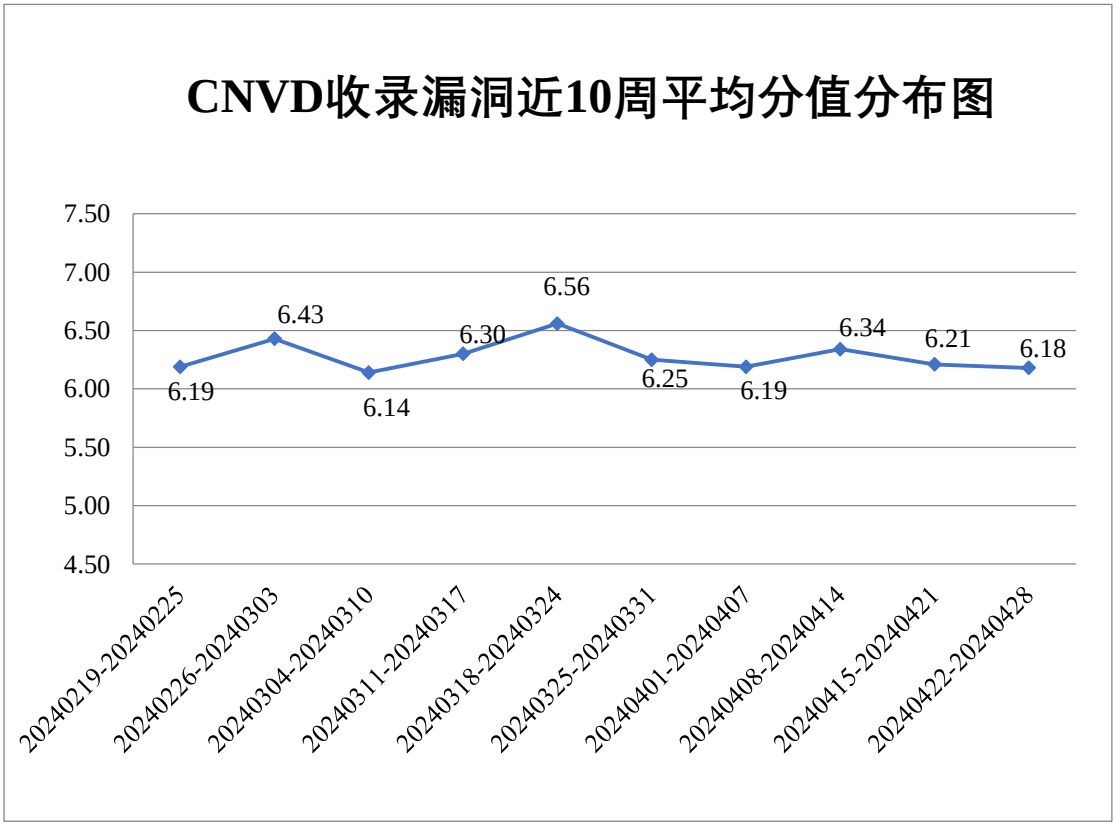

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 12 起，向基础电信企业通报漏洞事件 8 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 907 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 78 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 22 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：

重庆远秋科技股份有限公司、重庆森鑫炬科技有限公司、中科红旗（北京）信息科技有限公司、中地数码科技有限公司、智互联（深圳）科技有限公司、郑州金恒电子技术有限公司、正方软件股份有限公司、真珍斑马技术贸易（上海）有限公司、浙江安邦护卫科技服务有限公司、长沙乔伦科技有限公司、漳州市芗城帝兴软件开发有限公司、用友网络科技股份有限公司、雅马哈乐器音响（中国）投资有限公司、兄弟（中国）商业有限公司、新天科技股份有限公司、新都（青岛）电子有限公司、西安瑞友信息技术资讯有限公司、网件（北京）网络技术有限公司、万商云集（成都）科技股份有限公司、同望科技股份有限公司、天维尔信息科技股份有限公司、天津神州浩天科技有限公司、天津拂云科技有限公司、四平市九州易通科技有限公司、世邦通信股份有限公司、深圳市亿联智能有限公司、深圳市必联电子有限公司、上海易正软件技术服务有限公司、上海九慧信息科技有限公司、上海汉得信息技术股份有限公司、上海国位信息科技有限公司、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、山脉科技股份有限公司、山东潍微科技股份有限公司、厦门一指通智能科技有限公司、厦门四信通信科技有限公司、厦门四联信息技术有限公司、厦门科拓通讯技术股份有限公司、三星（中国）投资有限公司、瑞斯康达科技发展股份有限公司、融智通科技（北京）股份有限公司、麒麟软件有限公司、南京科远智慧科技集团股份有限公司、南京鼎华智能系统有限公司、迈普通信技术股份有限公司、龙采科技集团有限责任公司、理光（中国）投资有限公司、柯尼卡美能达办公系统（中国）有限公司、吉翁电子（深圳）有限公司、惠普贸易（上海）有限公司、弘扬软件股份有限公司、河北先河环保科技股份有限公司、杭州新视窗信息技术有限公司、杭州海康威视数字技术股份有限公司、海洋 CMS、桂林崇胜网络科技有限公司、广州市奥威亚电子科技有限公司、广东飞企互联科技股份有限公司、广东保伦电子股份有限公司、富士施乐（中国）有限公司、福建科立讯通信有限公司、东莞台昶电子有限公司、东莞市德诚软件科技有限公司、的卢信息技术（上海）有限公司、戴尔(中国)有限公司、北京星网锐捷网络技术有限公司、北京万户软件技术有限公司、北京通达信科科技有限公司、北京神州视翰科技有限公司、北京山石网科信息技术有限公司、北京普照天星科技有限公司、北京金和网络股份有限公司、北京百卓

网络技术有限公司、安美世纪（北京）科技有限公司、安科瑞电气股份有限公司、安徽中技国医医疗科技有限公司和爱普生（中国）有限公司。

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、北京启明星辰信息安全技术有限公司、阿里云计算有限公司、北京数字观星科技有限公司、北京升鑫网络科技有限公司（青藤云）等单位报送公开收集的漏洞数量较多。快页信息技术有限公司、河南东方云盾信息技术有限公司、内蒙古中叶信息技术有限责任公司、成都久信信息技术股份有限公司、北京山石网科信息技术有限公司、江苏金盾检测技术股份有限公司、北京卓识网安技术股份有限公司、北京中睿天下信息技术有限公司、江苏晟晖信息科技有限公司、北京微步在线科技有限公司、上海观安信息技术股份有限公司、广州安亿信软件科技有限公司、江苏锋刃信息科技有限公司、山东云天安全技术有限公司、安徽天行网安信息安全技术有限公司、中国工程物理研究院计算机应用研究所、中电福富信息科技有限公司、西藏熙安信息技术有限责任公司、陕西青山四纪信息技术有限公司、中国航天系统科学与工程研究院、上海亿保健康科技集团有限公司、 河南宝通信息安全测评有限公司、山石网科通信技术股份有限公司、中资网络信息安全科技有限公司、河南灵创电子科技有限公司、江苏极元信息技术有限公司、湖南泛联新安信息科技有限公司、杭州默安科技有限公司、甘肃赛飞安全科技有限公司及其他个人白帽子向 CNVD 提交了 7766 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）、三六零数字安全科技集团有限公司和上海交大向 CNVD 共享的白帽子报送的 6572 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）	3805	3805
奇安信网神（补天平台）	1951	1951
新华三技术有限公司	815	0
北京启明星辰信息安全技术有限公司	735	0
上海交大	422	422
三六零数字安全科技集团有限公司	394	394
阿里云计算有限公司	329	0
北京数字观星科技有	321	0

限公司		
北京升鑫网络科技有限公司（青藤云）	133	133
华为技术有限公司	106	0
恒安嘉新（北京）科技股份公司	103	0
深信服科技股份有限公司	102	1
北京知道创宇信息技术有限公司	60	0
杭州迪普科技股份有限公司	10	0
北京安信天行科技有限公司	4	4
北京长亭科技有限公司	3	2
北京神州绿盟科技有限公司	2	2
杭州安恒信息技术股份有限公司	1	1
中电科网络安全科技股份有限公司	1	1
北京智游网安科技有限公司	1	1
北京天融信网络安全技术有限公司	1	1
快页信息技术有限公司	61	61
河南东方云盾信息技术有限公司	56	56
内蒙古中叶信息技术有限责任公司	23	23
成都久信信息技术股份有限公司	14	14
北京山石网科信息技	12	12

术有限公司		
江苏金盾检测技术股份有限公司	9	9
北京卓识网安技术股份有限公司	8	8
北京中睿天下信息技术有限公司	4	4
江苏晟晖信息科技有限公司	4	4
北京微步在线科技有限公司	3	3
上海观安信息技术股份有限公司	2	2
广州安亿信软件科技有限公司	2	2
江苏锋刃信息科技有限公司	2	2
山东云天安全技术有限公司	2	2
安徽天行网安信息安全技术有限公司	2	2
中国工程物理研究院计算机应用研究所	2	2
中电福富信息科技有限公司	2	2
西藏熙安信息技术有限责任公司	2	2
陕西青山四纪信息技术有限公司	1	1
中国航天系统科学与工程研究院	1	1
上海亿保健康科技集团有限公司	1	1
河南宝通信息安全测评有限公司	1	1

山石网科通信技术股份有限公司	1	1
中资网络信息安全科技有限公司	1	1
河南灵创电子科技有限公司	1	1
江苏极元信息技术有限公司	1	1
湖南泛联新安信息科技有限公司	1	1
杭州默安科技有限公司	1	1
甘肃赛飞安全科技有限公司	1	1
西门子（中国）有限公司	1	0
CNCERT 宁夏分中心	8	8
CNCERT 贵州分中心	3	3
个人	816	816
报送总计	10348	7766

本周漏洞按类型和厂商统计

本周，CNVD 收录了 623 个漏洞。WEB 应用 219 个，应用程序 155 个，网络设备（交换机、路由器等网络端设备）117 个，智能设备（物联网终端设备）81 个，安全产品 26 个，数据库 13 个，操作系统 12 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	219
应用程序	155
网络设备（交换机、路由器等网络端设备）	117
智能设备（物联网终端设备）	81
安全产品	26
数据库	13
操作系统	12

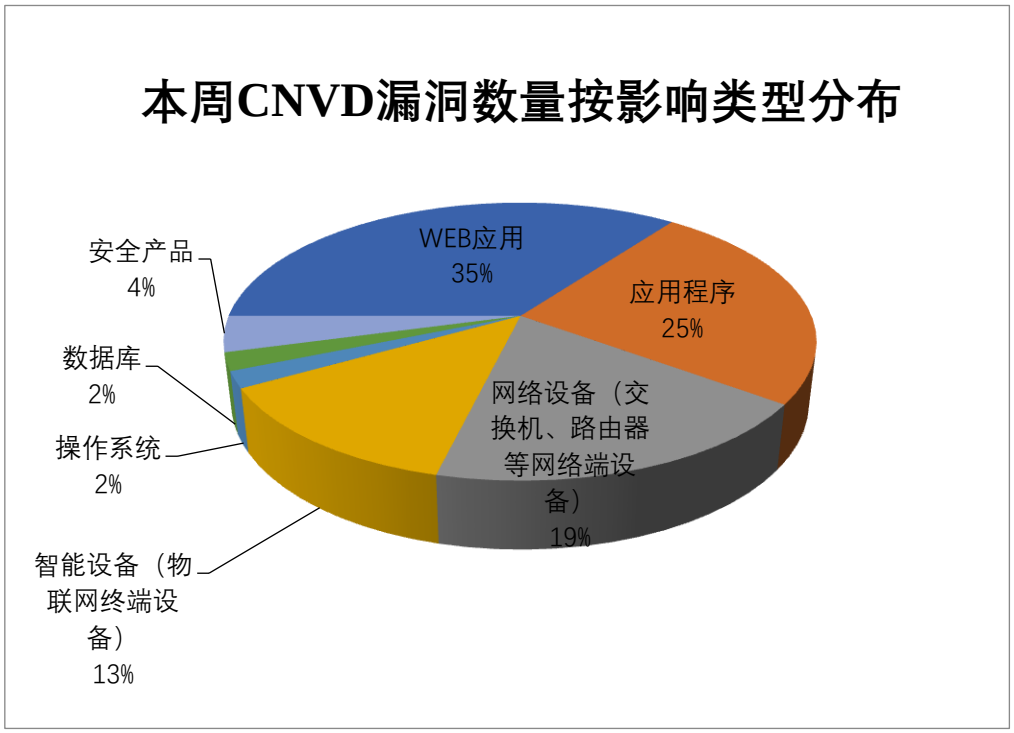

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及爱普生（中国）有限公司、IBM、Tenda 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	爱普生（中国）有限公司	27	5%
2	IBM	21	3%
3	Tenda	19	3%
4	Palo Alto Networks	18	3%
5	Adobe	18	3%
6	北京星网锐捷网络技术有限公司	15	3%
7	雅马哈乐器音响（中国）投资有限公司	14	2%
8	用友网络科技股份有限公司	14	2%
9	北京百卓网络技术有限公司	14	2%
10	其他	463	74%

本周行业漏洞收录情况

本周，CNVD 收录了 77 个电信行业漏洞，24 个移动互联网行业漏洞，10 个工控行

业漏洞（如下图所示）。其中，“TP-LINK AC1350/N300 命令执行漏洞、Tenda F1203 formSetCfm 方法缓冲区溢出漏洞”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/

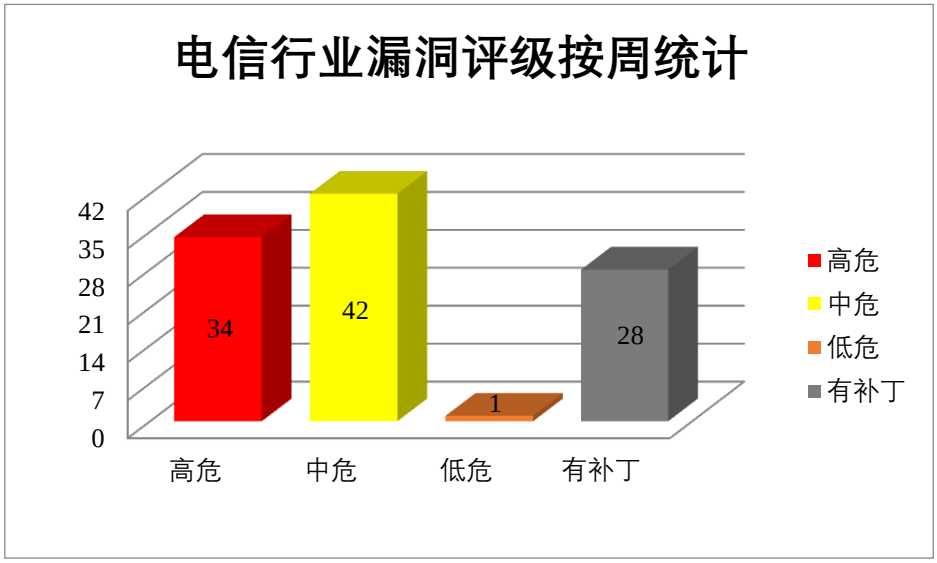

图 3 电信行业漏洞统计

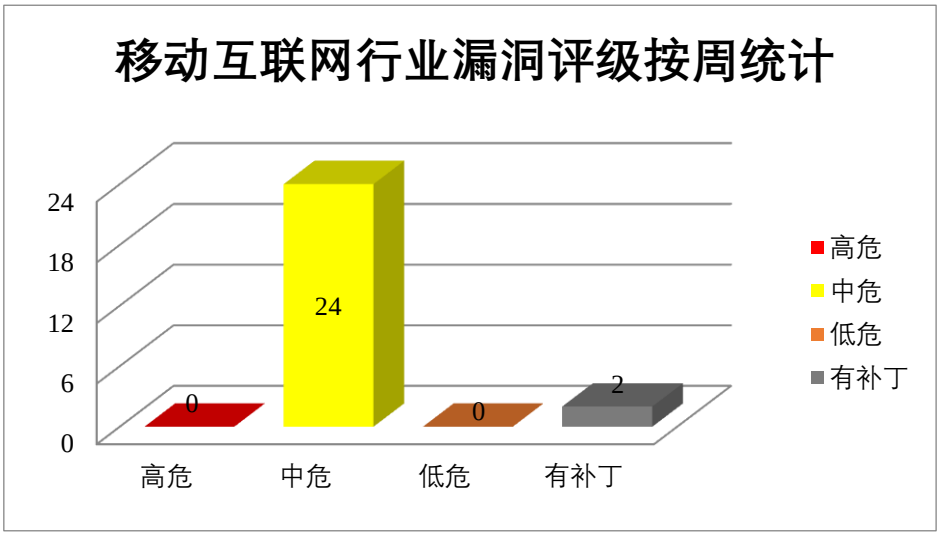

图 4 移动互联网行业漏洞统计

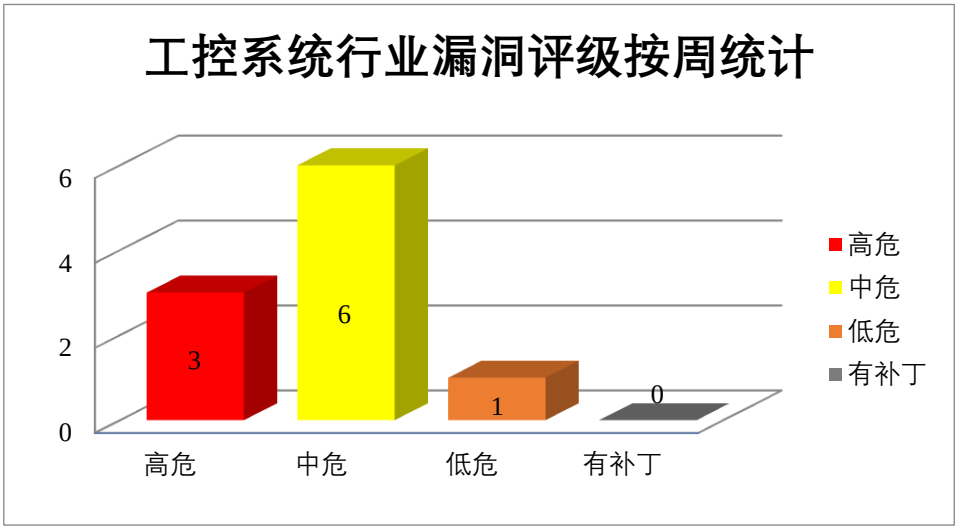

图 5 工控系统行业漏洞统计

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、Microsoft 产品安全漏洞

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 Defender for IoT 是一种适用于 IoT/OT 环境的资产发现、漏洞管理和威胁监控解决方案。 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 Update Stack 是美国微软（Microsoft）公司的用于管理更新的一部分。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拒绝服务，在服务器上执行任意代码，可以提升权限等。

CNVD 收录的相关漏洞包括：Microsoft Windows Hyper-V 拒绝服务漏洞（CNVD-2024-19326）、Microsoft Windows Hyper-V 远程代码执行漏洞（CNVD-2024-19327）、Microsoft Defender for IoT 远程代码执行漏洞（CNVD-2024-19328、CNVD-2024-19329）、Microsoft Defender for IoT 权限提升漏洞（CNVD-2024-19330、CNVD-2024-19331）、Microsoft Excel 远程代码执行漏洞（CNVD-2024-19332）、Microsoft Windows Update Stack 特权提升漏洞。其中，除“Microsoft Windows Hyper-V 拒绝服务漏洞（CNVD-2024-19326）、Microsoft Windows Update Stack 特权提升漏洞”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-2024-19326

https://www.cnvd.org.cn/flaw/show/CNVD-2024-19327

https://www.cnvd.org.cn/flaw/show/CNVD-2024-19328

https://www.cnvd.org.cn/flaw/show/CNVD-2024-19329

https://www.cnvd.org.cn/flaw/show/CNVD-2024-19330

https://www.cnvd.org.cn/flaw/show/CNVD-2024-19331

https://www.cnvd.org.cn/flaw/show/CNVD-2024-19332

https://www.cnvd.org.cn/flaw/show/CNVD-2024-20288

2、IBM 产品安全漏洞

IBM Security Verify Privilege 是美国国际商业机器（IBM）公司的一个解决方案，用于管理和保护用户的身份和权限。IBM SPSS Statistics 是美国国际商业机器（IBM）公司的一个软件包。用于交互式或批量统计分析。IBM WebSphere Application Server Liberty 是美国国际商业机器（IBM）公司的一款构建于 Open Liberty 项目之上的 Java 应用程序服务器。IBM Security Verify Access（ISAM）是美国国际商业机器（IBM）公司的一款提高用户访问安全的服务。该服务通过使用基于风险的访问、单点登录、集成访问管理控制、身份联合以及移动多因子认证实现对 Web、移动、IoT 和云技术等平台安全简单的访问。IBM Maximo Application Suite 是一组用于资产监控、管理、预测性维护和可靠性规划的应用程序。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞从 SOAP API 获取敏感信息，获取高度敏感的私有信息，使用特制的 HTTP 请求导致拒绝服务等。

CNVD 收录的相关漏洞包括：IBM Security Verify Privilege 信息泄露漏洞、IBM SPSS Statistics 资源管理错误漏洞、IBM Security Verify Access Appliance 和 IBM Application Gateway 信息泄露漏洞、IBM Security verify Access Appliance 拒绝服务漏洞、IBM WebSphere Application Server Liberty 加密问题漏洞、IBM WebSphere Application Server Liberty 资源管理错误漏洞（CNVD-2024-20495）、IBM Security verify Access Appliance 信任管理问题漏洞、IBM Maximo Application Suite 目录遍历漏洞。其中，“IBM Security Verify Privilege 信息泄露漏洞、IBM Security Verify Access Appliance 和 IBM Application Gateway 信息泄露漏洞、IBM Security verify Access Appliance 信任管理问题漏洞、IBM Maximo Application Suite 目录遍历漏洞”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-2024-19019

https://www.cnvd.org.cn/flaw/show/CNVD-2024-19027

https://www.cnvd.org.cn/flaw/show/CNVD-2024-19025

https://www.cnvd.org.cn/flaw/show/CNVD-2024-19024

https://www.cnvd.org.cn/flaw/show/CNVD-2024-19028

https://www.cnvd.org.cn/flaw/show/CNVD-2024-20495

https://www.cnvd.org.cn/flaw/show/CNVD-2024-20492

https://www.cnvd.org.cn/flaw/show/CNVD-2024-20497

3、 Adobe 产品安全漏洞

Adobe Animate 是美国奥多比（Adobe）公司的一套 Flash 动画制作软件。Adobe Bridge 是美国奥多比（Adobe）公司的一款文件查看器。Adobe After Effects 是美国奥多比（Adobe）公司的一套视觉效果和动态图形制作软件。该软件主要用于 2D 和 3D 合成、动画制作和视觉特效制作等。Adobe Illustrator 是美国奥多比（Adobe）公司的一套基于向量的图像制作软件。Adobe Commerce 是美国奥多比（Adobe）公司的一种面向商家和品牌的全球领先的数字商务解决方案。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞绕过 ASLR 等措施，系统崩溃，从而导致拒绝服务，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 Animate 缓冲区溢出漏洞（CNVD-2024-19000、CNVD-2024-19001）、Adobe Bridge 缓冲区溢出漏洞（CNVD-2024-18999）、Adobe Animate 代码问题漏洞（CNVD-2024-19003）、Adobe Animate 输入验证错误漏洞（CNVD-2024-19002）、Adobe After Effects 缓冲区溢出漏洞（CNVD-2024-19006）、Adobe Illustrator 缓冲区溢出漏洞（CNVD-2024-19005）、Adobe Commerce 输入验证错误漏洞（CNVD-2024-19008）。其中，“Adobe Animate 缓冲区溢出漏洞（CNVD-2024-19000）、Adobe Animate 输入验证错误漏洞（CNVD-2024-19002）、Adobe Illustrator 缓冲区溢出漏洞（CNVD-2024-19005）、Adobe Commerce 输入验证错误漏洞（CNVD-2024-19008）”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-2024-19000
https://www.cnvd.org.cn/flaw/show/CNVD-2024-18999
https://www.cnvd.org.cn/flaw/show/CNVD-2024-19003
https://www.cnvd.org.cn/flaw/show/CNVD-2024-19002
https://www.cnvd.org.cn/flaw/show/CNVD-2024-19001
https://www.cnvd.org.cn/flaw/show/CNVD-2024-19006
https://www.cnvd.org.cn/flaw/show/CNVD-2024-19005
https://www.cnvd.org.cn/flaw/show/CNVD-2024-19008

4、 Oracle 产品安全漏洞

Oracle MySQL 是美国甲骨文（Oracle）公司的一套开源的关系数据库管理系统。本周，上述产品被披露存在拒绝服务漏洞，攻击者可利用漏洞导致 MySQL 服务器挂起或频繁重复崩溃。

CNVD 收录的相关漏洞包括：Oracle MySQL 拒绝服务漏洞（CNVD-2024-19011、CNVD-2024-19010、CNVD-2024-19009、CNVD-2024-19014、CNVD-2024-19013、CNVD-2024-19012、CNVD-2024-19018、CNVD-2024-19017）。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-2024-19011
https://www.cnvd.org.cn/flaw/show/CNVD-2024-19010
https://www.cnvd.org.cn/flaw/show/CNVD-2024-19009
https://www.cnvd.org.cn/flaw/show/CNVD-2024-19014
https://www.cnvd.org.cn/flaw/show/CNVD-2024-19013
https://www.cnvd.org.cn/flaw/show/CNVD-2024-19012
https://www.cnvd.org.cn/flaw/show/CNVD-2024-19018
https://www.cnvd.org.cn/flaw/show/CNVD-2024-19017

5、Tenda W18E 缓冲区溢出漏洞

Tenda W18E 是中国腾达（Tenda）公司的一款无线路由器。本周，Tenda W18E 被披露存在缓冲区溢出漏洞。攻击者可利用该漏洞在系统上执行任意代码或者导致拒绝服务。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-2024-20280

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

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-2024-20267	ZenML 目录遍历漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://security.samsungmobile.com/serviceWeb.smsb?year=2024&month=03
CNVD-2024-20285	TP-LINK AC1350 拒绝服务漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.tp-link.com/us/support/download/eap115/v4/#Firmware
CNVD-2024-20284	TP-LINK AC1350 和 N300 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://www.tp-link.com/us/support/download/eap115/v4/#Firmware
CNVD-2024-20294	WordPress WP Fusion Lite 插件远程代码执行漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：https://wordpress.org/plugins/wp-fusion-lite/
CNVD-2024-20299	Tenda AC15 固件栈缓冲区溢出漏洞	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.tendacn.com/us/download/detail-3851.html

CNVD-2024-20296	Tenda F1203 formQuickIndex 方法缓冲区溢出漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://wordpress.org/plugins/eventprime-event-calendar-management/
CNVD-2024-20301	Tenda AC10 缓冲区溢出漏洞（CNVD-2024-20301）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://freeimage.sourceforge.io/
CNVD-2024-20307	Foxit PDF Reader 远程代码执行漏洞（CNVD-2024-20307）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.foxit.com/support/security-bulletins.html
CNVD-2024-20432	Palo Alto Networks PAN-OS 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://security.paloaltonetworks.com/CVE-2024-3400
CNVD-2024-20599	Foxit PDF Reader 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://www.foxit.com/support/security-bulletins.html

小结：本周，Microsoft 产品被披露存在多个漏洞，攻击者可利用漏洞导致拒绝服务，在服务器上执行任意代码，可以提升权限。此外，IBM、Adobe、Oracle 等多款产品被披露存在多个漏洞，攻击者可利用漏洞从 SOAP API 获取敏感信息，获取高度敏感的私有信息，使用特制的 HTTP 请求导致拒绝服务，在当前用户的上下文中执行任意代码等等。另外，Tenda W18E 被披露存在缓冲区溢出漏洞。攻击者可利用漏洞在系统上执行任意代码或者导致拒绝服务。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、Online Courseware editt.php 文件跨站脚本漏洞

验证描述

Online Courseware 是一个在线课件系统。

Online Courseware 1.0 版本存在跨站脚本漏洞，该漏洞源于 editt.php 文件的 id 参数对用户提供的数据缺乏有效过滤与转义，攻击者可利用该漏洞通过注入精心设计的有效载荷执行任意 Web 脚本或 HTML。

验证信息

POC 链接：https://github.com/thisissuperann/Vul/blob/Online-Courseware/Online-Courseware-11.md

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2024-20289

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. 蠕虫爆发，PlugX 新变种感染 250 万主机

PlugX 是有着十多年历史的老牌恶意软件（蠕虫病毒），最早可追溯到 2008 年，最初只被亚洲的黑客组织使用，主要针对政府、国防、技术和政治组织。

参考链接：https://www.secrss.com/articles/65628

2. Glints 数据泄露：新加坡招聘平台敏感员工数据涉嫌泄露

据称，一名暗网用户泄露了一个数据库，其中包含与新加坡在线招聘平台 Glints 相关的员工记录。2024 年 4 月 23 日报道的 Glints 数据泄露事件被添加到一个暗网论坛中，样本数据被泄露，特别突出了敏感的员工信息。

参考链接：https://thecyberexpress.com/glints-data-breach/

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