国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2024 年 02 月 19 日-2024 年 02 月 25 日 **2024 年第 8 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 330 个，其中高危漏洞 121 个、中危漏洞 185 个、低危漏洞 24 个。漏洞平均分值为 6.19。本周收录的漏洞中，涉及 0day 漏洞 203 个（占 62%），其中互联网上出现“POSCMS 跨站脚本漏洞、GreenCMS 跨站脚本漏洞”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 6129 个，与上周（7723 个）环比减少 21%。

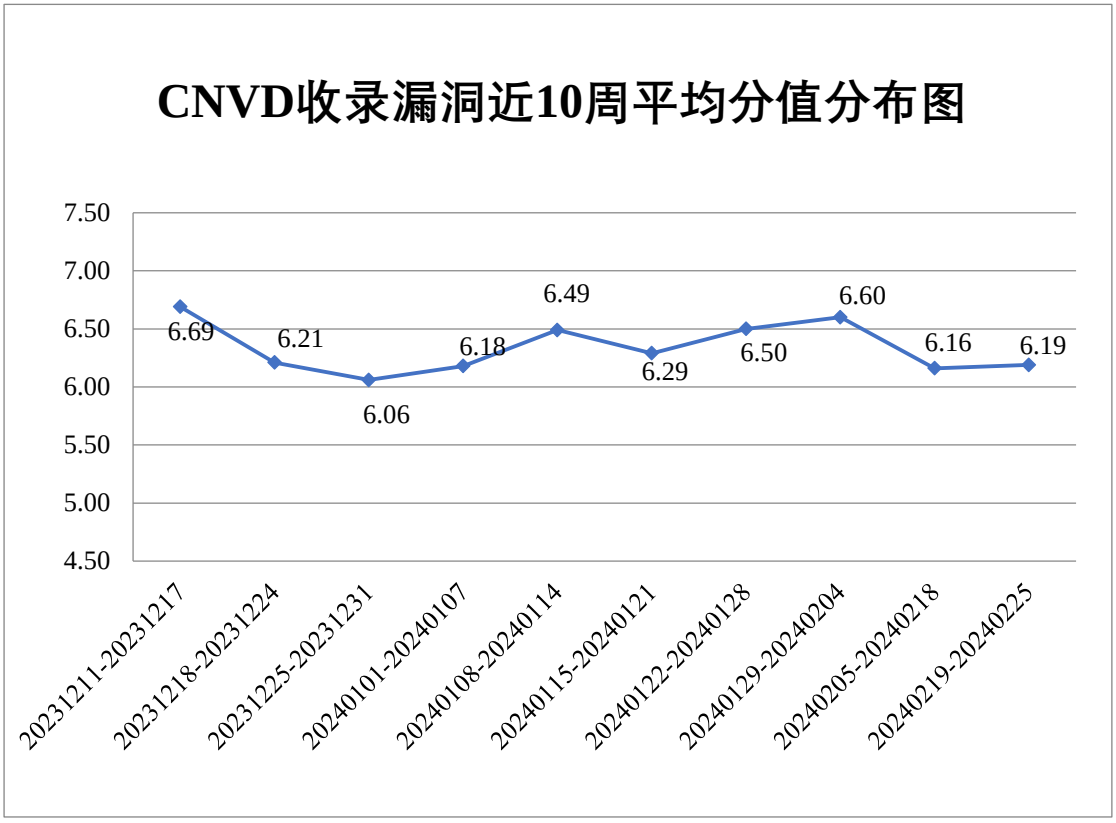

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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，协调 CNCERT 各分中心验证和处置涉及地方重要部门漏洞事件 697 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 119 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 34 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：

珠海金山办公软件有限公司、郑州市景安网络科技股份有限公司、浙江宇视科技有限公司、浙江汉脑数码科技有限公司、浙江大华技术股份有限公司、浙江阿拉丁信息科技股份有限公司、掌如科技服务有限公司、长沙市云研网络科技有限公司、友讯电子设备（上海）有限公司、用友网络科技股份有限公司、兄弟（中国）商业有限公司、新华三技术有限公司、西门子（中国）有限公司、西安众邦网络科技有限公司、武汉达梦数据库有限公司、威海市天罡仪表股份有限公司、万洲电气股份有限公司、统信软件技术有限公司、腾讯安全应急响应中心、神州数码集团股份有限公司、深圳市中电数通智慧安全科技股份有限公司、深圳市赢家服饰有限公司、深圳市同享软件科技有限公司、深圳市蓝凌软件股份有限公司、深圳市捷顺科技实业股份有限公司、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、深圳市鼎游信息技术有限公司、深圳市博思高科技有限公司、上海卓卓网络科技有限公司、上海迅饶自动化科技有限公司、上海威派格智慧水务股份有限公司、上海商汤智能科技有限公司、上海琪派软件有限公司、上海牛之云科技有限公司、上海寰创通信科技股份有限公司、上海华测导航技术股份有限公司、上海泛微网络科技股份有限公司、上海博达数据通信有限公司、上海爱数信息技术股份有限公司、山西森甲能源科技有限公司、山西点可云科技有限公司、山石网科通信技术股份有限公司、山东潍微科技股份有限公司、厦门亿联网络技术股份有限公司、厦门四信通信科技有限公司、厦门四联信息技术有限公司、三星（中国）投资有限公司、青岛积成电子股份有限公司、青岛海信网络科技股份有限公司、普联技术有限公司、脑谋深算科技（广州）有限公司、龙采科技集团有限责任公司、联奕科技股份有限公司、浪潮电子信息产业股份有限公司、蓝卓数字科技有限公司、蓝网科技股份有限公司、快云信息科技有限公司、凯硕科技股份有限公司、金蝶软件（中国）有限公司-PSIRT、江西智博环境技术有限公司、江苏天瑞仪器股份有限公司、吉翁电子（深圳）有限公司、惠普贸易（上海）有限公司、湖南建研信息技术股份有限公司、宏脉信息技术（广州）股份有限公司、杭州中宝科技有限公司、杭州云天软件股份有限公司、杭州云润科技有限公司、杭州萤石网络股份有限公司、杭州雄伟科技开发股份有限公司、杭州瑞利声电技术有限公司、杭州品茗信息技术有限公司、杭州海康威视数字技术股份有限公司、杭州迪普科技股份有限公司、广州市保伦电子有限公司、广联达科技股份有限公司、广东全程云科技有限公司、广东飞企互联科技股份有限公司、福建星网智慧科技有限公司、

福建科立讯通信有限公司、东华软件股份公司、承德热力集团有限责任公司、北京致远互联软件股份有限公司、北京用友政务软件股份有限公司、北京永洪商智科技有限公司、北京亿赛通科技发展有限责任公司、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、北京小桔科技有限公司、北京希瑞亚斯科技有限公司、北京万户软件技术有限公司、北京通达信科科技有限公司、北京勤云科技发展有限公司、北京玛格泰克科技发展有限公司、北京朗新天霁软件技术有限公司、北京金和网络股份有限公司、北京宏景世纪软件股份有限公司、北京高校邦数字科技有限公司、北京百卓网络技术有限公司、北京百度网讯科技有限公司、北京安华金和科技有限公司、安徽生命港湾信息技术有限公司、爱普生（中国）有限公司、阿帕数字技术有限公司、阿里巴巴集团安全应急响应中心和华为技术有限公司。

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，北京启明星辰信息安全技术有限公司、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、北京神州绿盟科技有限公司等单位报送公开收集的漏洞数量较多。江苏金盾检测技术股份有限公司、联想集团、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、内蒙古洞明科技有限公司、贵州多彩网安科技有限公司、安徽天行网安信息安全技术有限公司、快页信息技术有限公司、中孚安全技术有限公司、西藏熙安信息技术有限责任公司、安徽锋刃信息科技有限公司、甘肃赛飞安全科技有限公司、北京微步在线科技有限公司、江苏晟晖信息科技有限公司、湖南泛联新安信息科技有限公司、北京中关村实验室、上海直画科技有限公司、任子行网络技术股份有限公司、含光实验室、杭州默安科技有限公司、江苏极元信息技术有限公司、广州安亿信软件科技有限公司、北京天下信安技术有限公司、海南神州希望网络有限公司、苏州棱镜七彩信息科技有限公司、博智安全科技股份有限公司、国网上海市电力公司、北京星网锐捷网络技术有限公司、内蒙古中叶信息技术有限责任公司、杭州中正检测技术有限公司、河南灵创电子科技有限公司、江苏云天网络安全技术有限公司及其他个人白帽子向 CNVD 提交了 6129 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、奇安信网神（补天平台）和三六零数字安全科技集团有限公司向 CNVD 共享的白帽子报送的 5089 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
北京启明星辰信息安全技术有限公司	2101	10
斗象科技（漏洞盒子）	1840	1840

上海交大	1489	1489
奇安信网神（补天平台）	1260	1260
三六零数字安全科技集团有限公司	500	500
深信服科技股份有限公司	360	0
安天科技集团股份有限公司	358	0
北京数字观星科技有限公司	255	0
北京神州绿盟科技有限公司	231	0
天津市国瑞数码安全系统股份有限公司	184	0
阿里云计算有限公司	162	0
北京知道创宇信息技术有限公司	81	0
恒安嘉新（北京）科技股份公司	61	0
中国电信集团系统集成有限责任公司	24	0
北京安信天行科技有限公司	16	16
杭州安恒信息技术股份有限公司	15	5
杭州迪普科技股份有限公司	10	0
北京智游网安科技有限公司	4	4
远江盛邦（北京）网络安全科技股份有限公司	1	1
南京联成科技发展股份有限公司	1	1

江苏金盾检测技术股份有限公司	82	82
联想集团	51	51
奇安星城网络安全运营服务（长沙）有限公司	31	31
西门子（中国）有限公司	28	0
河南东方云盾信息技术有限公司	24	24
内蒙古洞明科技有限公司	21	21
贵州多彩网安科技有限公司	19	19
安徽天行网安信息安全技术有限公司	7	7
快页信息技术有限公司	6	6
中孚安全技术有限公司	5	5
西藏熙安信息技术有限责任公司	5	5
安徽锋刃信息科技有限公司	4	4
甘肃赛飞安全科技有限公司	4	4
北京微步在线科技有限公司	4	4
江苏晟晖信息科技有限公司	3	3
湖南泛联新安信息科技有限公司	3	3
北京中关村实验室	3	3
上海直画科技有限公司	3	3

任子行网络技术股份有限公司	3	3
含光实验室	2	2
杭州默安科技有限公司	2	2
江苏极元信息技术有限公司	2	2
广州安亿信软件科技有限公司	2	2
北京天下信安技术有限公司	2	2
海南神州希望网络有限公司	2	2
苏州棱镜七彩信息科技有限公司	2	2
博智安全科技股份有限公司	2	2
国网上海市电力公司	1	1
北京星网锐捷网络技术有限公司	1	1
内蒙古中叶信息技术有限责任公司	1	1
杭州中正检测技术有限公司	1	1
河南灵创电子科技有限公司	1	1
江苏云天网络安全技术有限公司	1	1
CNCERT 河北分中心	3	3
CNCERT 湖南分中心	1	1
个人	699	699
报送总计	9984	6129

本周漏洞按类型和厂商统计

本周，CNVD 收录了 330 个漏洞。WEB 应用 143 个，应用程序 127 个，网络设备（交换机、路由器等网络端设备）33 个，智能设备（物联网终端设备）14 个，操作系统 8 个，数据库 3 个，安全产品 2 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	143
应用程序	127
网络设备（交换机、路由器等网络端设备）	33
智能设备（物联网终端设备）	14
操作系统	8
数据库	3
安全产品	2

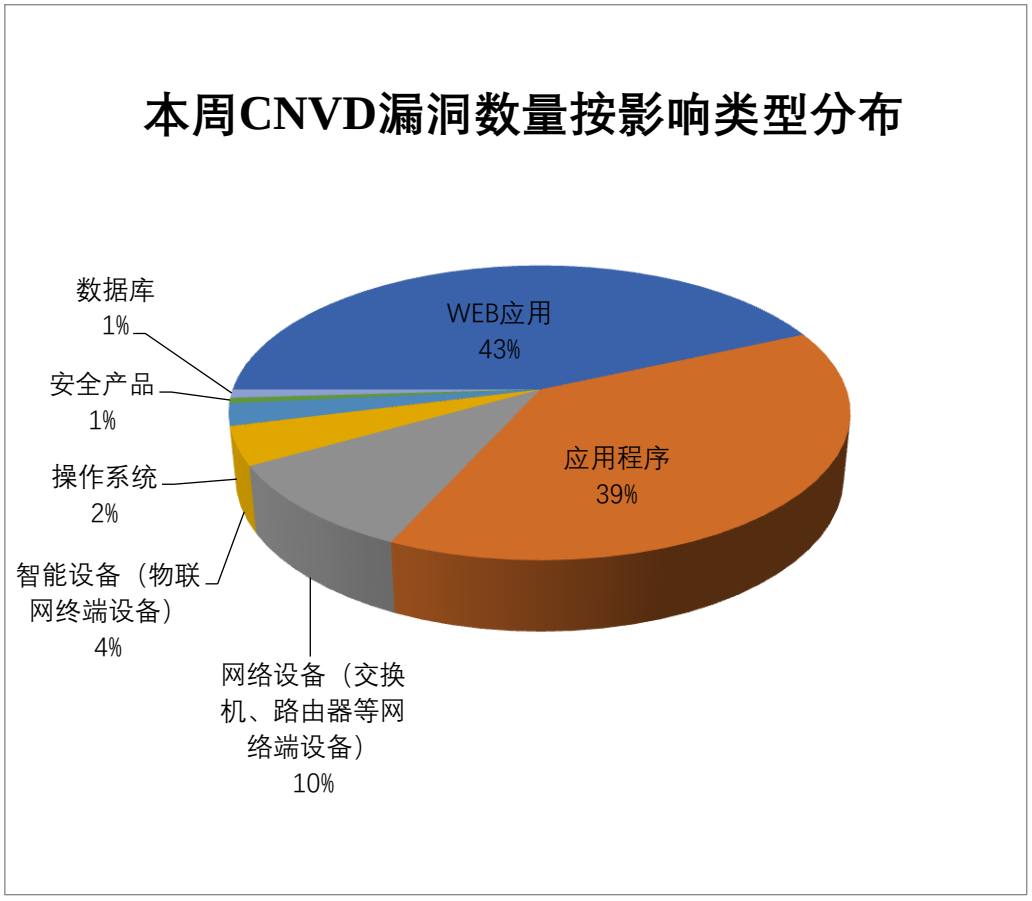

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Siemens、Dell、IBM 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	Siemens	28	9%

2	Dell	19	6%
3	IBM	14	4%
4	Adobe	13	4%
5	Fortinet	12	4%
6	北京星网锐捷网络技术有限公司	11	3%
7	openBI	9	3%
8	ZFCMS	8	2%
9	用友网络科技股份有限公司	7	2%
10	其他	209	63%

本周行业漏洞收录情况

本周，CNVD 收录了 16 个电信行业漏洞，22 个移动互联网行业漏洞，6 个工控行业漏洞（如下图所示）。其中，“TOTOLINK N200RE loginAuth 函数缓冲区溢出漏洞、Samsung Exynos baseband 输入验证错误漏洞”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/

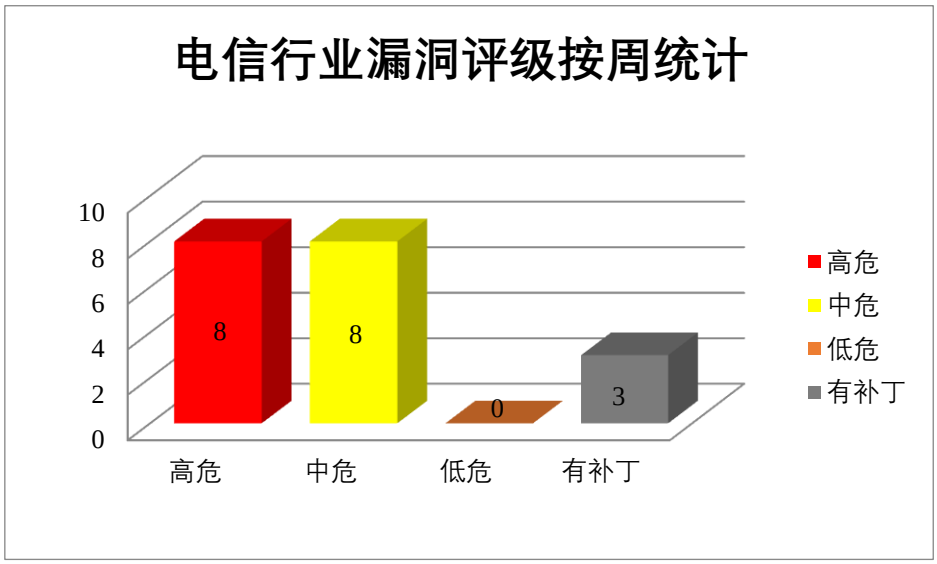

图 3 电信行业漏洞统计

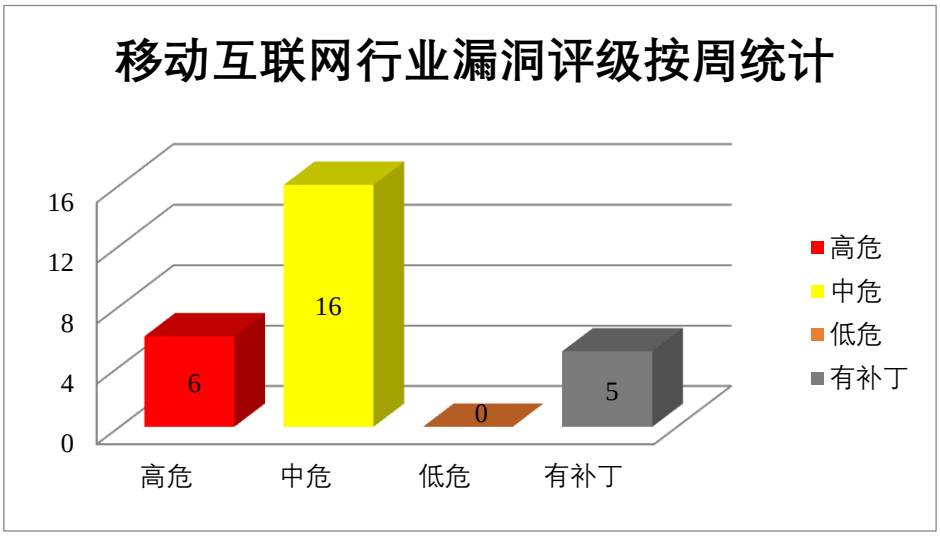

图 4 移动互联网行业漏洞统计

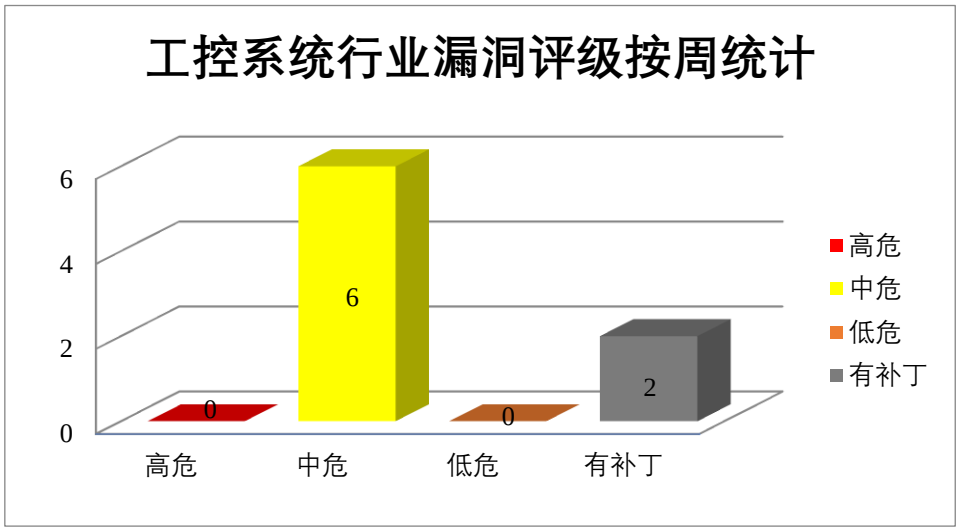

图 5 工控系统行业漏洞统计

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、 Adobe 产品安全漏洞

Adobe ColdFusion 是美国奥多比（Adobe）公司的一套快速应用程序开发平台。该平台包括集成开发环境和脚本语言。Adobe Framemaker 是美国奥多比（Adobe）公司的一套用于编写和编辑大型或复杂文档（包括结构化文档）的页面排版软件。Adobe Photoshop 是一个由 Adobe 开发和发行的应用软件，用于图像处理。Adobe Animate 是由 Adobe 公司开发的多媒体创作和电脑动画程序，可用于设计矢量图形和动画。Adobe Substance 3D Painter 是美国奥多比（Adobe）公司的一个 3D 纹理处理应用程序。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞导致安全功能绕过，提交特殊的请求，可在应用程序上下文执行任意代码等。

CNVD 收录的相关漏洞包括：Adobe ColdFusion 反序列化漏洞（CNVD-2024-09606、CNVD-2024-09607）、Adobe ColdFusion 反序列化代码执行漏洞、Adobe FrameMaker 身份验证错误漏洞、Adobe Photoshop 缓冲区溢出漏洞（CNVD-2024-09611）、Adobe Animate 缓冲区溢出漏洞（CNVD-2024-09610）、Adobe Substance 3D Painter 缓冲区溢出漏洞（CNVD-2024-09898、CNVD-2024-09899）。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-2024-09606

https://www.cnvd.org.cn/flaw/show/CNVD-2024-09605

https://www.cnvd.org.cn/flaw/show/CNVD-2024-09604

https://www.cnvd.org.cn/flaw/show/CNVD-2024-09607

https://www.cnvd.org.cn/flaw/show/CNVD-2024-09611

https://www.cnvd.org.cn/flaw/show/CNVD-2024-09610

https://www.cnvd.org.cn/flaw/show/CNVD-2024-09898

https://www.cnvd.org.cn/flaw/show/CNVD-2024-09899

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 FortiOS 是美国飞塔（Fortinet）公司的一套专用于 FortiGate 网络安全平台上的安全操作系统。该系统为用户提供防火墙、防病毒、IPSec/SSLVPN、Web 内容过滤和反垃圾邮件等多种安全功能。Fortinet FortiIsolator 是美国飞塔（Fortinet）公司的一个为浏览器提供远程安全隔离功能的应用。该应用为 Fortinet Security Fabric 添加了额外的高级威胁防护功能，并保护关键业务数据免受网络上复杂威胁的侵害。来自 Web 的内容和文件在远程容器中访问，然后将无风险的内容呈现给用户。Fortinet FortiSandbox 是美国飞塔（Fortinet）公司的一款 APT（高级持续性威胁）防护设备。该设备提供双重沙盒技术、动态威胁智能系统、实时控制面板和报告等功能。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 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、schema 中毒等攻击的威胁。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特制的 HTTP 或 HTTPS 请求提升权限，提交特殊的请求，可在应用程序上下文执行任意 os 命令等。

CNVD 收录的相关漏洞包括：Fortinet FortiADC 授权问题漏洞（CNVD-2024-09277）、Fortinet FortiOS and FortiProxy 授权问题漏洞、Fortinet FortiIsolator 命令执行漏洞、Fortinet FortiSandbox 跨站脚本漏洞（CNVD-2024-09278）、Fortinet FortiNAC 权限提升漏洞（CNVD-2024-09283）、Fortinet FortiOS 授权问题漏洞（CNVD-2024-09281）、Fortinet FortiWeb 命令注入漏洞（CNVD-2024-09285）、Fortinet FortiNAC 命令注

入漏洞（CNVD-2024-09284）。其中，除“Fortinet FortiIsolator 命令执行漏洞、Fortinet FortiSandbox 跨站脚本漏洞（CNVD-2024-09278）、Fortinet FortiNAC 权限提升漏洞（CNVD-2024-09283）”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-2024-09277
https://www.cnvd.org.cn/flaw/show/CNVD-2024-09274
https://www.cnvd.org.cn/flaw/show/CNVD-2024-09279
https://www.cnvd.org.cn/flaw/show/CNVD-2024-09278
https://www.cnvd.org.cn/flaw/show/CNVD-2024-09283
https://www.cnvd.org.cn/flaw/show/CNVD-2024-09281
https://www.cnvd.org.cn/flaw/show/CNVD-2024-09285
https://www.cnvd.org.cn/flaw/show/CNVD-2024-09284

3、 Siemens 产品安全漏洞

SINEC NMS 是面向数字化企业的新一代网络管理系统(NMS)。Tecnomatix Plant Simulation 可对物流系统及其流程进行建模、模拟、探索和优化。这些模型可以在生产执行之前对从全球生产设施到当地工厂和特定生产线的所有制造计划进行物料流、资源利用和物流分析。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞在服务器数据库上执行任意 SQL 查询，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 SINEC NMS 任意文件上传漏洞、Siemens SINEC NMS SQL 注入漏洞（CNVD-2024-09309）、Siemens Tecnomatix Plant Simulation 越界写入漏洞（CNVD-2024-09320）、Siemens Tecnomatix Plant Simulation 越界读取漏洞（CNVD-2024-09321）、Siemens Tecnomatix Plant Simulation 缓冲区溢出漏洞（CNVD-2024-09319、CNVD-2024-09327、CNVD-2024-09326、CNVD-2024-09325）。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-2024-09308
https://www.cnvd.org.cn/flaw/show/CNVD-2024-09309
https://www.cnvd.org.cn/flaw/show/CNVD-2024-09320
https://www.cnvd.org.cn/flaw/show/CNVD-2024-09319
https://www.cnvd.org.cn/flaw/show/CNVD-2024-09321
https://www.cnvd.org.cn/flaw/show/CNVD-2024-09327
https://www.cnvd.org.cn/flaw/show/CNVD-2024-09326
https://www.cnvd.org.cn/flaw/show/CNVD-2024-09325

4、 Dell 产品安全漏洞

Dell Unity 是一款统一的混合存储阵列，适用于本地和云中的通用工作负载。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞以 root 权限执行命令。

CNVD 收录的相关漏洞包括：Dell Unity 命令注入漏洞（CNVD-2024-09151、CNVD-2024-09154、CNVD-2024-09153、CNVD-2024-09152、CNVD-2024-09157、CNVD-2024-09156、CNVD-2024-09155、CNVD-2024-09160）。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-2024-09151
https://www.cnvd.org.cn/flaw/show/CNVD-2024-09154
https://www.cnvd.org.cn/flaw/show/CNVD-2024-09153
https://www.cnvd.org.cn/flaw/show/CNVD-2024-09152
https://www.cnvd.org.cn/flaw/show/CNVD-2024-09157
https://www.cnvd.org.cn/flaw/show/CNVD-2024-09156
https://www.cnvd.org.cn/flaw/show/CNVD-2024-09155
https://www.cnvd.org.cn/flaw/show/CNVD-2024-09160

5、openBI 反序列化漏洞

openBI 是 openBI 公司的一个大数据可视化解决方案。本周，openBI 被披露存在反序列化漏洞。攻击者可利用此漏洞导致代码执行。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-2024-09293

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-2024-09178	IBM SOAR QRadar Plugin App 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://www.ibm.com/support/pages/node/7111679
CNVD-2024-09273	GPAC 缓冲区溢出漏洞（CNVD-2024-09273）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/gpac/gpac/commit/7aef8038c6bdd310e65000704e39afaa0e721048
CNVD-2024-09292	openBI Icon.php 文件存在任意文件上传漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：http://openbi.com/
CNVD-2024-09290	IBM Security Access Manager Container 资源管理错误漏	高	厂商已发布了漏洞修复程序，请及时关注更新：

	洞		https://www.ibm.com/support/pages/node/7106586
CNVD-2024-09296	TOTOLINK A3300R setWiFiScheduleCfg 方法命令注入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.totolink.net/home/menu/detail/menu_listtpl/download/id/241/ids/36.html
CNVD-2024-09295	TOTOLINK A3300R setIpv6Cfg 方法命令注入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.totolink.net/home/menu/detail/menu_listtpl/download/id/241/ids/36.html
CNVD-2024-09300	openBI 操作系统命令注入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：http://openbi.com/
CNVD-2024-09299	openBI Upload.php 文件任意文件上传漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：http://openbi.com/
CNVD-2024-09304	Tenda i9 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://www.tendacn.com/download/detail-3477.html
CNVD-2024-09307	Siemens SINEC NMS 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://cert-portal.siemens.com/productcert/html/ssa-943925.html

小结：本周，Adobe 产品被披露存在多个漏洞，攻击者可利用漏洞导致安全功能绕过，提交特殊的请求，可以应用程序上下文执行任意代码等。此外，Fortinet、Siemens、Dell 等多款产品被披露存在多个漏洞，攻击者可利用漏洞通过特制的 HTTP 或 HTTPS 请求提升权限，提交特殊的请求，可在应用程序上下文执行任意 os 命令等。另外，openBI 被披露存在反序列化漏洞。攻击者可利用此漏洞导致代码执行。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、POSCMS 跨站脚本漏洞

验证描述

POSCMS 是一个内容管理系统。

POSCMS v4.6.2 版本存在跨站脚本漏洞。该漏洞源于应用对用户提供的数据缺乏有

效过滤与转义，攻击者可利用漏洞在/index.php?c=install&m=index&step=2&is_install_db=0 中加载特制 payload，进而执行任意代码。

验证信息

POC 链接：https://github.com/Num-Nine/CVE/issues/12

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2024-09302

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. 苹果推出后量子加密协议 PQ3，iMessage 即将迎来大升级

近期，苹果公布了一种新的 iMessage 后量子加密协议，称为 PQ3。PQ3 具有抗妥协加密和广泛的防御功能，可以“针对高度复杂的量子攻击提供广泛的防御”。

参考链接：https://thehackernews.com/2024/02/apple-unveils-pq3-protocol-post-quantum.html

2. 德国电池制造商 Varta AG 因网络攻击仍未恢复生产

据外媒报道，在检测到其系统受到网络攻击近两周后，德国电池制造商 Varta AG 仍未恢复其工厂的生产。该公司生产各种用于家用和工业用途的电池和存储产品，包括锂离子小型化电池和移动电源。

参考链接：http://www.anquan419.com/knews/24/6636.html

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