国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2024 年 07 月 15 日-2024 年 07 月 21 日　　2024 年第 29 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 351 个，其中高危漏洞 174 个、中危漏洞 168 个、低危漏洞 9 个。漏洞平均分值为 6.80。本周收录的漏洞中，涉及 0day 漏洞 246 个（占 70%），其中互联网上出现“OpenPLC 跨站脚本漏洞、Z-BlogPHP 跨站脚本漏洞（CNVD-2024-32984）”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 14074 个，与上周（19961）环比减少 29%。

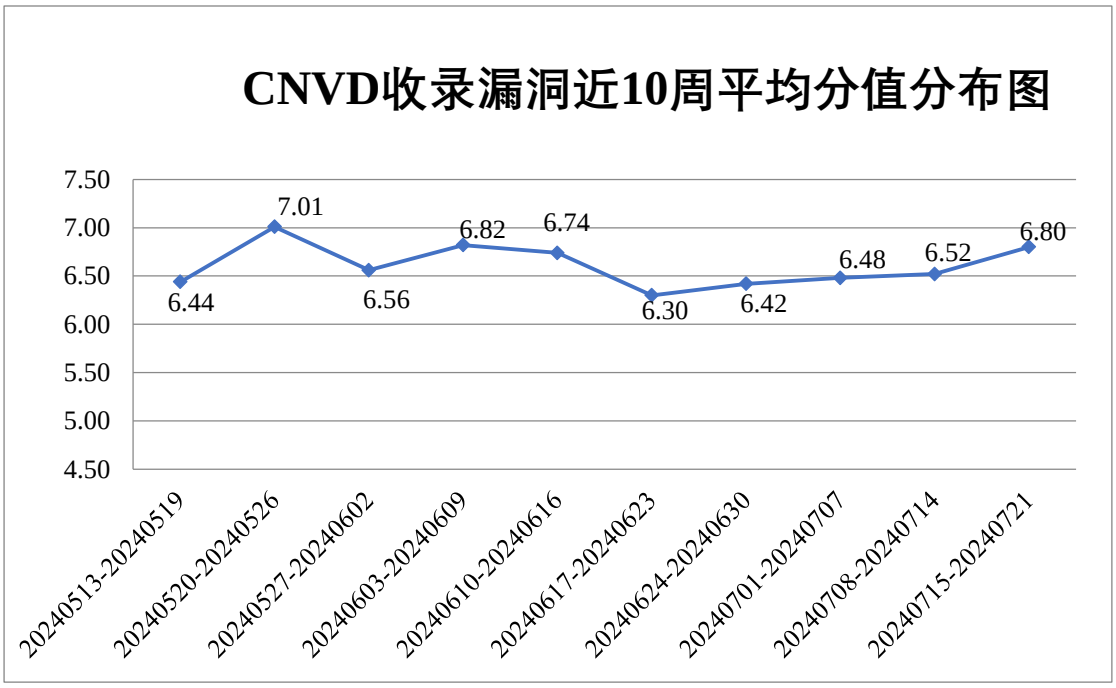

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 4 起，向基础电信

企业通报漏洞事件 2 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 813 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 91 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 10 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：

重庆中联信息产业有限责任公司、智石开工业软件有限公司、智互联（深圳）科技有限公司、智恒科技股份有限公司、浙江中控技术股份有限公司、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、新天科技股份有限公司、西安众邦网络科技有限公司、西安大西信息科技有限公司、潍坊家园驿站电子技术有限公司、万洲电气股份有限公司、天津南大通用数据技术股份有限公司、深圳市云迅通科技股份有限公司、深圳市赛格导航科技股份有限公司、深圳市蓝凌软件股份有限公司、深圳市吉祥腾达科技有限公司、深圳市必联电子有限公司、深圳科士达科技股份有限公司、深圳警翼智能科技股份有限公司、深圳华视美达信息技术有限公司、上海商派网络科技有限公司、上海桑锐电子科技股份有限公司、上海甲鼎信息技术有限公司、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、上海百胜软件股份有限公司、上海爱数信息技术股份有限公司、山东潍微科技股份有限公司、山东领图信息科技股份有限公司、山东聚恒网络技术有限公司、厦门悦讯信息科技股份有限公司、厦门微信软件有限公司、厦门市索联软件科技有限公司、厦门纳龙健康科技股份有限公司、赛蓝（广州）信息技术有限公司、融智通科技（北京）股份有限公司、日冲商业(北京)有限公司、任子行网络技术股份有限公司、青岛三利集团有限公司、青岛和正信息技术有限公司、青岛海威茨仪表有限公司、麒麟软件有限公司、迈普通信技术股份有限公司、京师博仁（北京）科技发展股份公司、江苏麦维智能科技有限公司、佳能（中国）有限公司、吉翁电子（深圳）有限公司、杭州叙简科技股份有限公司、杭州雄伟科技开发股份有限公司、杭州三汇信息工程有限公司、杭州恒生数字设备科技有限公司、杭州海康威视数字技术股份有限公司、杭州短链网络技术有限公司、国子软件股份有限公司、广州市坚信信息科技有限公司、广州安网通信技术有限公司、富士胶片商业创新（中国）有限公司、成都太航科技有限公司、成都极企科技有限公司、畅捷通信息技术股份有限公司、比亚迪股份有限公司、北京中创视讯科技有限公司、北京中成科信科技发展有限公司、北京致远互联软件股份有限公司、北京易普行科技有限公司、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、北京微控工业网关技术有限公司、北京网御星云信息技术有限公司、北京万户网络技术有限公司、北京神州视翰科技有限公司、北京润乾信息系统技术有限公司、北京人大金仓信息技术股份有限公司、北京龙软科技股份有限公司、北京凯特伟业科技有限公司、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、北京凤凰世纪科技有限公司、安微协达软件科技有限公司、安美世纪（北京）科技有限公司、shopex_software 和 GAC

R&D Cybersecurity Pentest Team。

本周，CNVD 发布了《Oracle 发布 2024 年 7 月的安全公告》，详情参见 CNVD 网站公告内容（https://www.cnvd.org.cn/webinfo/show/10226）。

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、北京神州绿盟科技有限公司、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等单位报送公开收集的漏洞数量较多。河南东方云盾信息技术有限公司、江苏金盾检测技术股份有限公司、江苏云天网络安全技术有限公司、快页信息技术有限公司、马鞍山书拓安全科技有限公司、重庆都会信息科技有限公司、成都卫士通信息安全技术有限公司、山东云天安全技术有限公司、江苏百达智慧网络科技有限公司、安徽天行网安信息安全技术有限公司、上海直画科技有限公司、河南灵创电子科技有限公司、江苏锋刃信息科技有限公司、北京远禾科技有限公司、联想集团、广州华南检验检测中心有限公司、江苏极元信息技术有限公司、福建福诺移动通信技术有限公司、西藏闪锁网络科技有限公司、厦门聚丁科技有限公司、海南神州希望网络有限公司、成都久信信息技术股份有限公司、北京航空航天大学、赛尔网络有限公司、平安银河实验室、北京中睿天下信息技术有限公司、贵州蓝天创新科技有限公司、江西中和证信息安全技术有限公司、江苏国保信息系统测评中心有限公司、北京小桔科技有限公司、北京山石网科信息技术有限公司及其他个人白帽子向 CNVD 提交了 14074 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）、三六零数字安全科技集团有限公司、斗象科技（漏洞盒子）和上海交大向 CNVD 共享的白帽子报送的 12940 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	原创漏洞数量
斗象科技（漏洞盒子）	10002	10002
奇安信网神（补天平台）	2158	2158
新华三技术有限公司	792	0
北京神州绿盟科技有限公司	663	1
深信服科技股份有限公司	548	0
安天科技集团股份有限公司	496	0
三六零数字安全科技	406	406

集团有限公司		
上海交大	374	374
北京数字观星科技有限公司	374	0
天津市国瑞数码安全系统股份有限公司	195	0
阿里云计算有限公司	165	0
恒安嘉新（北京）科技股份公司	166	0
北京天融信网络安全技术有限公司	150	0
北京启明星辰信息安全技术有限公司	69	0
北京安信天行科技有限公司	52	52
北京知道创宇信息技术有限公司	48	1
京东科技信息技术有限公司	43	0
杭州迪普科技股份有限公司	30	0
杭州安恒信息技术股份有限公司	30	19
远江盛邦（北京）网络安全科技股份有限公司	26	26
南京众智维信息科技有限公司	17	17
北京长亭科技有限公司	1	1
河南东方云盾信息技术有限公司	52	52
江苏金盾检测技术股份有限公司	34	34
江苏云天网络安全技	18	18

术有限公司		
快页信息技术有限公司	12	12
马鞍山书拓安全科技有限公司	9	9
重庆都会信息科技有限公司	9	9
成都卫士通信息安全技术有限公司	9	9
山东云天安全技术有限公司	4	4
江苏百达智慧网络科技有限公司	3	3
安徽天行网安信息安全技术有限公司	3	3
上海直画科技有限公司	3	3
河南灵创电子科技有限公司	3	3
江苏锋刃信息科技有限公司	3	3
北京远禾科技有限公司	3	3
联想集团	2	2
广州华南检验检测中心有限公司	2	2
江苏极元信息技术有限公司	2	2
福建福诺移动通信技术有限公司	2	2
西藏闪锁网络科技有限公司	2	2
厦门聚丁科技有限公司	2	2
海南神州希望网络有	2	2

限公司		
成都久信信息技术股份有限公司	2	2
北京航空航天大学	1	1
赛尔网络有限公司	1	1
平安银河实验室	1	1
北京中睿天下信息技术有限公司	1	1
贵州蓝天创新科技有限公司	1	1
江西中和证信息安全技术有限公司	1	1
江苏国保信息系统测评中心有限公司	1	1
北京小桔科技有限公司	1	1
北京山石网科信息技术有限公司	1	1
CNCERT 河北分中心	1	1
个人	826	826
报送总计	17822	14074

本周漏洞按类型和厂商统计

本周，CNVD 收录了 351 个漏洞。WEB 应用 185 个，应用程序 80 个，网络设备（交换机、路由器等网络端设备）53 个，智能设备（物联网终端设备）25 个，数据库 4 个，操作系统 2 个，安全产品 1 个，车联网 1 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	185
应用程序	80
网络设备（交换机、路由器等网络端设备）	53
智能设备（物联网终端设备）	25
数据库	4
操作系统	2
安全产品	1
车联网	1

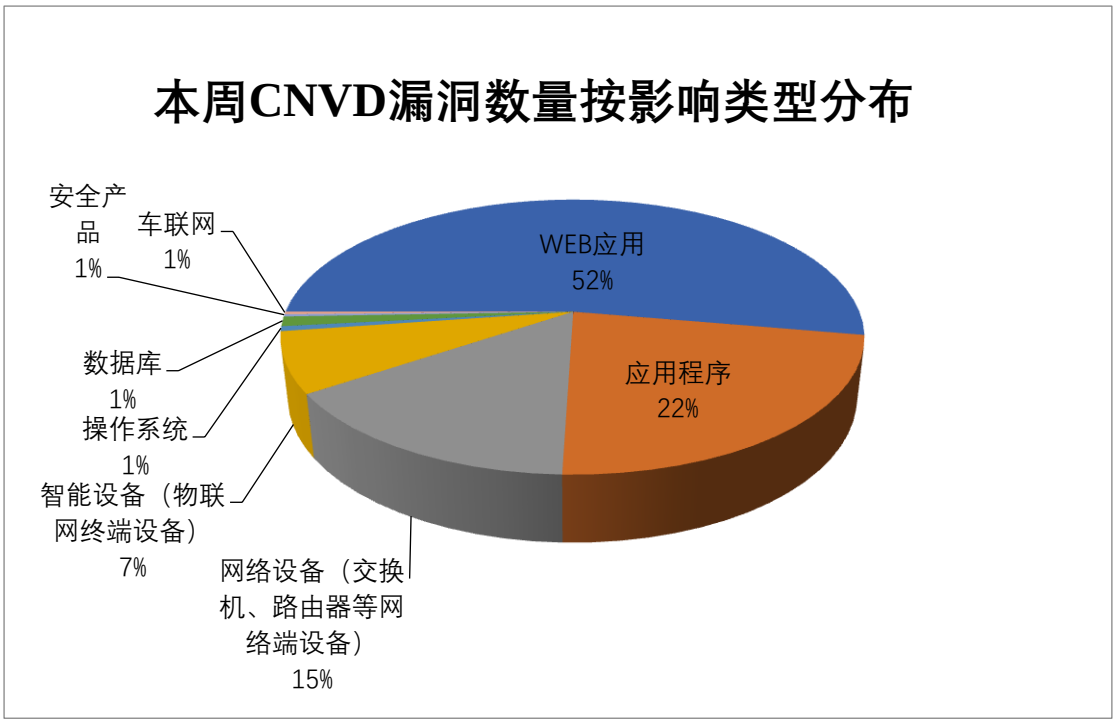

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Autodesk、J2eeFAST、Adobe 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	Autodesk	20	6%
2	J2eeFAST	16	5%
3	Adobe	12	3%
4	D-Link	12	3%
5	Siemens	11	3%
6	Microsoft	11	3%
7	北京神州视翰科技有限公司	10	3%
8	北京金和网络股份有限公司	10	3%
9	Ruvar	10	3%
10	其他	239	68%

本周行业漏洞收录情况

本周，CNVD 收录了 19 个电信行业漏洞，17 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，“Delta Electronics CNCSoft-G2 越界读取漏洞、Delta

Electronics CNCSoft-G2 缓冲区溢出漏洞（CNVD-2024-32986）”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/

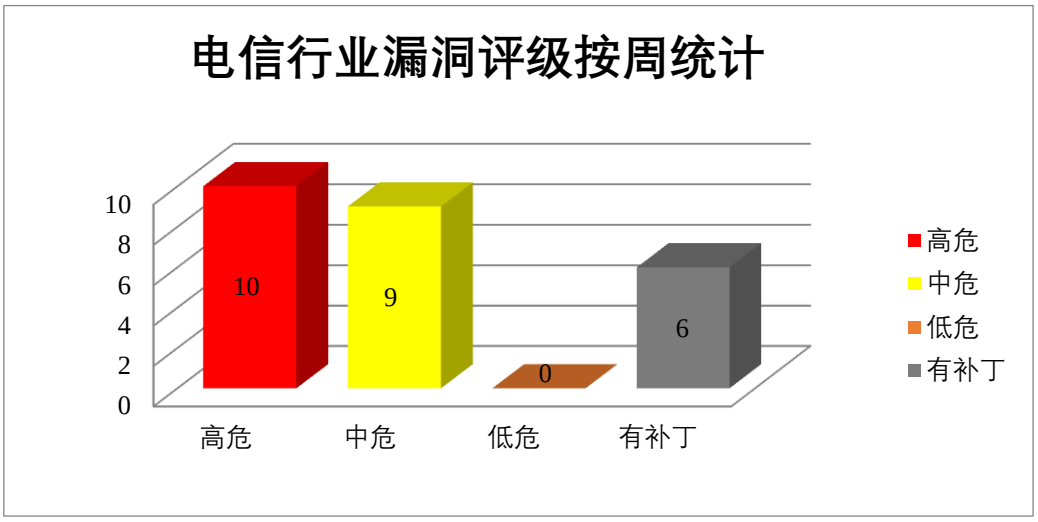

图 3 电信行业漏洞统计

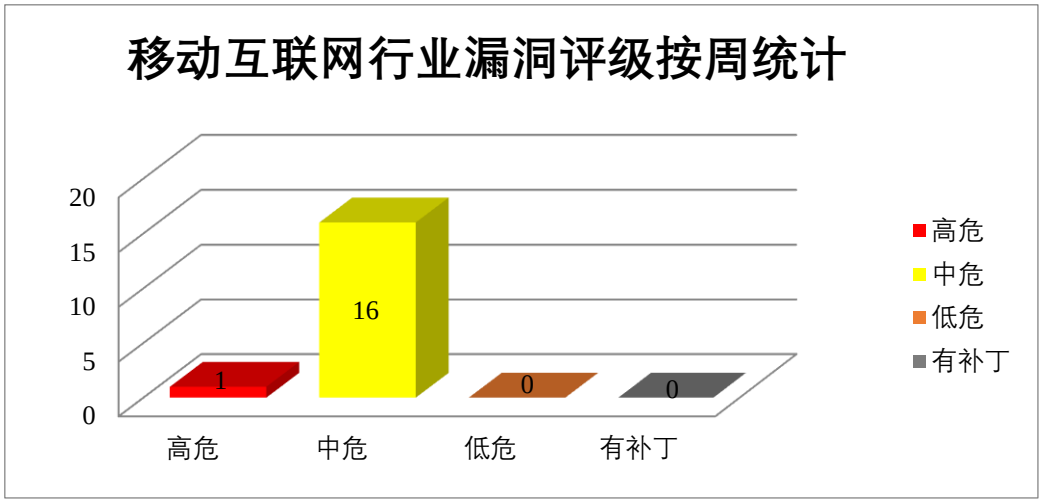

图 4 移动互联网行业漏洞统计

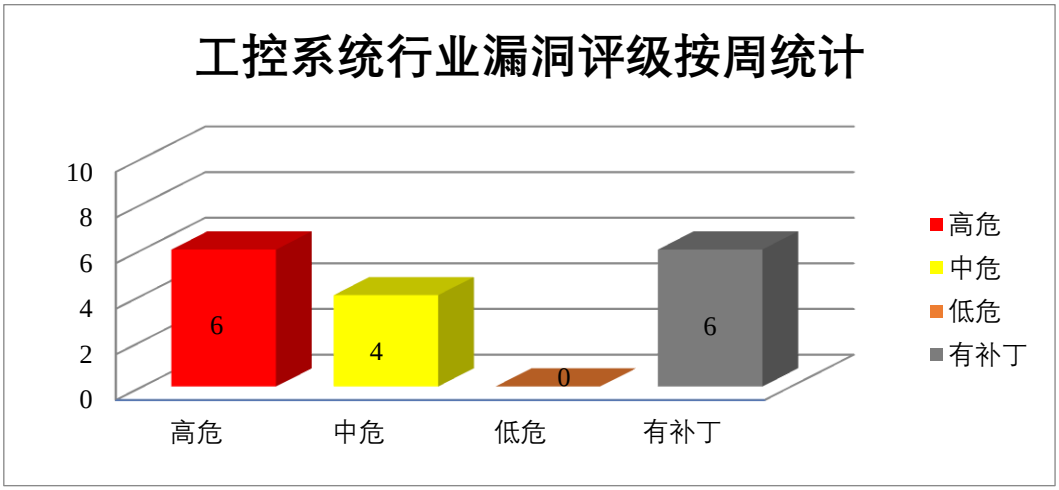

图 5 工控系统行业漏洞统计

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 Experience Manager（AEM）是美国奥多比（Adobe）公司的一套可用于构建网站、移动应用程序和表单的内容管理解决方案。该方案支持移动内容管理、营销销售活动管理和多站点管理等。本周，上述产品被披露存在跨站脚本漏洞，攻击者可利用漏洞通过注入精心设计的有效载荷执行任意 Web 脚本或 HTML。

CNVD 收录的相关漏洞包括：Adobe Experience Manager 跨站脚本漏洞（CNVD-2024-32819、CNVD-2024-32818、CNVD-2024-32817、CNVD-2024-32822、CNVD-2024-32821、CNVD-2024-32820、CNVD-2024-32826、CNVD-2024-33255）。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-2024-32819

https://www.cnvd.org.cn/flaw/show/CNVD-2024-32818

https://www.cnvd.org.cn/flaw/show/CNVD-2024-32817

https://www.cnvd.org.cn/flaw/show/CNVD-2024-32822

https://www.cnvd.org.cn/flaw/show/CNVD-2024-32821

https://www.cnvd.org.cn/flaw/show/CNVD-2024-32820

https://www.cnvd.org.cn/flaw/show/CNVD-2024-32826

https://www.cnvd.org.cn/flaw/show/CNVD-2024-33255

2、 Microsoft 产品安全漏洞

Microsoft Windows Secure Boot 是美国微软（Microsoft）公司的安全启动。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安全功能。

CNVD 收录的相关漏洞包括：Microsoft Windows Secure Boot 安全特性绕过漏洞、Microsoft Windows Secure Boot 安全功能绕过漏洞（CNVD-2024-32546、CNVD-2024-32545、CNVD-2024-32544、CNVD-2024-32547、CNVD-2024-32552、CNVD-2024-32551、CNVD-2024-32550）。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-2024-32543
https://www.cnvd.org.cn/flaw/show/CNVD-2024-32546
https://www.cnvd.org.cn/flaw/show/CNVD-2024-32545
https://www.cnvd.org.cn/flaw/show/CNVD-2024-32544
https://www.cnvd.org.cn/flaw/show/CNVD-2024-32547
https://www.cnvd.org.cn/flaw/show/CNVD-2024-32552
https://www.cnvd.org.cn/flaw/show/CNVD-2024-32551
https://www.cnvd.org.cn/flaw/show/CNVD-2024-32550

3、 Siemens 产品安全漏洞

Siemens JT Open Toolkit（Siemens JTTK）是德国西门子（Siemens）公司的一个C++应用程序编程接口（API）。PLM XML SDK 是一种轻量级、灵活的产品数据传输机制。它支持一种基于适配器的方法，将来自任何源的数据转换为 XML 表示。SIMATIC PCS neo 是一种分布式控制系统（DCS）。SIMATIC STEP 7（TIA Portal）是一款用于配置和编程 SIMATIC 控制器的工程软件。Totally Integrated Automation Portal（TIA Portal）是一款 PC 软件，可提供西门子数字化自动化服务的完整范围，从数字规划、集成工程到透明操作。SINEMA Remote Connect 是一个用于远程网络的管理平台，能够简单管理总部、服务技术人员和已安装机器或工厂之间的隧道连接（VPN）。Siemens SINEMA Remote Connect Server 是一套远程网络管理平台。该平台主要用于远程访问、维护、控制和诊断底层网络。Mendix Encryption 模块负责以下加密需求：纯文本加密（例如密码）和 FileDocument 加密（例如文件或照片）。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞造成类型混淆，并在受影响的应用程序中执行任意代码等。

CNVD 收录的相关漏洞包括：Siemens JT Open 和 PLM 堆栈缓冲区溢出漏洞、Siemens SIMATIC STEP 7 (TIA Portal)反序列化漏洞、Siemens SINEMA Remote Connect Client 命令注入漏洞（CNVD-2024-32684、CNVD-2024-32685、CNVD-2024-32686）、Siemens SINEMA Remote Connect Server 命令注入漏洞（CNVD-2024-32688、CNVD-2024-32689）、Siemens Mendix Encryption 模块硬编码默认加密密钥漏洞。其中，除“Siemens SINEMA Remote Connect Client 命令注入漏洞（CNVD-2024-32684、CNVD-2024-32686）”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-2024-32682

https://www.cnvd.org.cn/flaw/show/CNVD-2024-32683

https://www.cnvd.org.cn/flaw/show/CNVD-2024-32684

https://www.cnvd.org.cn/flaw/show/CNVD-2024-32685

https://www.cnvd.org.cn/flaw/show/CNVD-2024-32686

https://www.cnvd.org.cn/flaw/show/CNVD-2024-32688

https://www.cnvd.org.cn/flaw/show/CNVD-2024-32689

https://www.cnvd.org.cn/flaw/show/CNVD-2024-32690

4、D-Link 产品安全漏洞

D-Link DAP-2622 是中国友讯（D-Link）公司的一款无线路由器。本周，上述产品被披露存在缓冲区溢出漏洞，攻击者可利用漏洞在根上下文中执行代码。

CNVD 收录的相关漏洞包括：D-Link DAP-2622 缓冲区溢出漏洞（CNVD-2024-32554、CNVD-2024-32558、CNVD-2024-32557、CNVD-2024-32556、CNVD-2024-32555、CNVD-2024-32561、CNVD-2024-32560、CNVD-2024-32559）。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-2024-32554

https://www.cnvd.org.cn/flaw/show/CNVD-2024-32558

https://www.cnvd.org.cn/flaw/show/CNVD-2024-32557

https://www.cnvd.org.cn/flaw/show/CNVD-2024-32556

https://www.cnvd.org.cn/flaw/show/CNVD-2024-32555

https://www.cnvd.org.cn/flaw/show/CNVD-2024-32561

https://www.cnvd.org.cn/flaw/show/CNVD-2024-32560

https://www.cnvd.org.cn/flaw/show/CNVD-2024-32559

5、ASUS RT-AX88U 缓冲区溢出漏洞

ASUS RT-AX88U 是中国华硕（ASUS）公司的一个无线路由器。本周，ASUS RT-AX88U 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-2024-33178

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-2024-32549	Microsoft Windows Secure Boot 安全功能绕过漏洞（CNVD-2024-32549）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-37987
CNVD-2024-32553	D-Link DAP-2622 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://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10349
CNVD-2024-32562	D-Link DAP-2622 缓冲区溢出漏洞（CNVD-2024-32562）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://supportannouncement.us.dlink.com/announcement/publication.aspx?name=SAP10349
CNVD-2024-32827	ServiceNow 模板注入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://support.servicenow.com/kb?id=kb_article_view&sysparm_article=KB1644293
CNVD-2024-32988	Delta Electronics CNCSoft-G2 缓冲区溢出漏洞（CNVD-2024-32988）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://downloadcenter.deltaww.com/en-US/DownloadCenter?v=1&q=cncsoft&sort_expr=cdate&sort_dir=DESC
CNVD-2024-32987	Delta Electronics CNCSoft-G2 越界写入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://downloadcenter.deltaww.com/en-US/DownloadCenter?v=1&q=cncsoft&sort_expr=cdate&sort_dir=DESC
CNVD-2024-32997	Autodesk AutoCAD 越界写入漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.autodesk.com/trust/security-advisories/adsk-sa-2024-0010
CNVD-2024-32996	Autodesk AutoCAD 内存错误引用漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.autodesk.com/trust/security-advisories/adsk-sa-2024-0009
CNVD-2024-32995	Autodesk AutoCAD 内存破坏漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.autodesk.com/trust/security-advisories/adsk-sa-2024-0009
CNVD-2024	Autodesk AutoCAD 越界读取	高	厂商已发布了漏洞修复程序，请及

-32994	漏洞		时关注更新：https://www.autodesk.com/trust/security-advisories/adsk-sa-2024-0009

小结：本周，Adobe 产品被披露存在跨站脚本漏洞，攻击者可利用漏洞通过注入精心设计的有效载荷执行任意 Web 脚本或 HTML。此外，Microsoft、Siemens、D-Link 等多款产品被披露存在多个漏洞，攻击者可利用漏洞绕过安全功能，造成类型混淆，在根上下文中执行代码等。另外，ASUS RT-AX88U 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、Z-BlogPHP 跨站脚本漏洞（CNVD-2024-32984）

验证描述

Z-BlogPHP 是 Z-blog 社区的一套开源的基于 PHP 的博客系统。

Z-BlogPHP 存在跨站脚本漏洞，攻击者可利用该漏洞通过精心制作的有效负载执行任意 web 脚本或 HTML。

验证信息

POC 链接：https://github.com/5r1an/CVE-2024-39203/issues/1

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2024-32984

信息提供者

北京长亭科技有限公司

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. CISA、FBI 警告操作系统命令注入漏洞

网络安全和基础设施安全局（CISA）和 FBI 发布了一项重要警报，敦促软件开发人员专注于消除允许未经授权的用户在操作系统（OS）上运行有害命令的弱点。

参考链接：https://www.anquanke.com/post/id/298012

2. SolarWinds 修复了访问权限审计软件中的 8 个关键缺陷

Access Rights Manager 是企业环境中的关键工具，可帮助管理员管理和审核其组织 IT 基础架构中的访问权限，以最大程度地减少威胁影响。

参考链接：https://www.bleepingcomputer.com/news/security/solarwinds-fixes-8-critical-bu

gs-in-access-rights-audit-software/

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