国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2024 年 12 月 30 日-2025 年 1 月 05 日 **2025 年第 1 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 247 个，其中高危漏洞 120 个、中危漏洞 117 个、低危漏洞 10 个。漏洞平均分值为 6.54。本周收录的漏洞中，涉及 0day 漏洞 184 个（占 74%），其中互联网上出现“JFinalCMS 跨站请求伪造漏洞（CNVD-2024-49644）、 ClassCMS 代码注入漏洞”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 22622 个，与上周（29176 个）环比减少 22%。

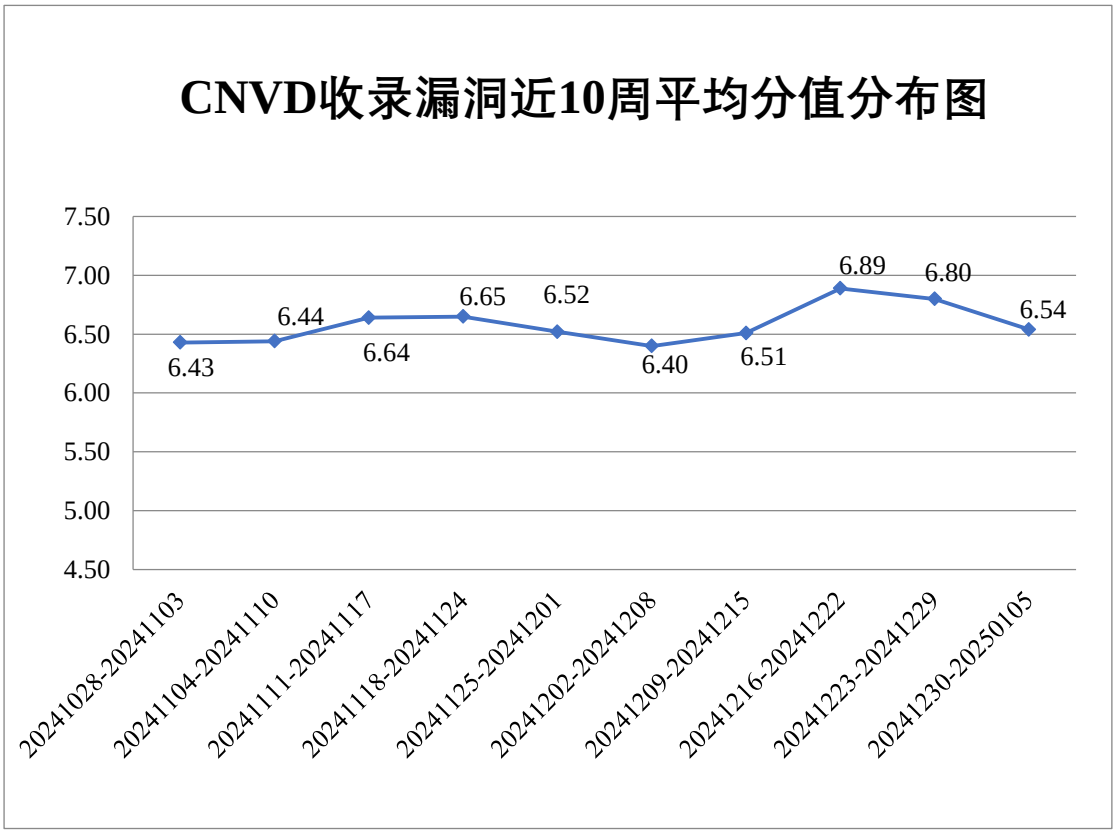

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 6 起，向基础电信企业通报漏洞事件 1 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 340 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 20 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 13 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：

紫光股份有限公司、重庆中联信息产业有限责任公司、中控技术股份有限公司、中电科金仓（北京）科技股份有限公司、郑州时空智友信息技术有限公司、浙江中控技术股份有限公司、浙江禾川科技股份有限公司、用友网络科技股份有限公司、信呼、西安瑞友信息技术资讯有限公司、无锡信捷电气股份有限公司、万洲电气股份有限公司、统信软件技术有限公司、天闻数媒科技（北京）有限公司、天津环球磁卡集团有限公司、深圳竹云科技股份有限公司、深圳市亿玛信诺科技有限公司、深圳市吉祥腾达科技有限公司、深圳市大世同舟信息科技有限公司、深圳勤杰软件有限公司、深圳达实智能股份有限公司、申瓯通信设备有限公司、上海新致软件股份有限公司、上海汇道信息科技有限公司、山东点狮信息科技有限公司、厦门正航软件科技有限公司、厦门微信软件有限公司、厦门美图网科技有限公司、厦门科拓通讯技术股份有限公司、青岛海信网络科技股份有限公司、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、利盟信息技术（中国）有限公司、柯尼卡美能达集团、江苏群杰物联科技有限公司、江苏汉思未来信息科技有限公司、吉翁电子（深圳）有限公司、湖南众合百易信息技术有限公司、湖南壹拾捌号网络技术有限公司、杭州雄伟科技开发股份有限公司、杭州海康威视数字技术股份有限公司、瀚高基础软件股份有限公司、广州市天翎网络科技有限公司、广州华壹智能科技有限公司、广东保伦电子股份有限公司、富士施乐（中国）有限公司、东芝（中国）有限公司、东莞市同享软件科技有限公司、大连华天软件有限公司、畅捷通信息技术股份有限公司、比亚迪股份有限公司、北京中庆现代技术股份有限公司、北京中关村科金技术有限公司、北京致远互联软件股份有限公司、北京炎黄盈动科技发展有限责任公司、北京亚控科技发展有限公司、北京天润融通科技股份有限公司、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、北京趋势威尔网络技术有限公司、北京敲敲云科技有限公司、北京龙软科技股份有限公司、北京金和网络股份有限公司、北京好雨科技有限公司、百度安全应急响应中心和安付宝商务有限公司。

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，深信服科技股份有限公司、新华三技术有限公司、北京天融信网络安全技术有限公司、北京数字观星科技有限公司、京东科技信息技术有限公司等单位报送公开收集的漏洞数量较多。江苏云天网络安全技术有限公司、北京时代新威信息技术有限公司、北京山石网科信息技术有限公司、山东正中信息技术股份有限公司、贵州多彩网安科技有限公司、北京远禾科技有限公司、北京天下信安技术有限公司及其他个人白帽子向 CNVD 提交了 22622 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 22413 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
奇安信网神（补天平台）	14373	14373
斗象科技（漏洞盒子）	5752	5752
三六零数字安全科技集团有限公司	1826	1826
深信服科技股份有限公司	871	0
新华三技术有限公司	475	0
上海交大	462	462
北京天融信网络安全技术有限公司	319	4
北京数字观星科技有限公司	229	0
京东科技信息技术有限公司	228	0
安天科技集团股份有限公司	174	0
阿里云计算有限公司	163	0
中国电信集团系统集成有限责任公司	60	0
北京启明星辰信息安全技术有限公司	59	0
北京知道创宇信息技术有限公司	50	0
北京长亭科技有限公	21	0

司		
南京众智维信息科技有限公司	17	5
北京安信天行科技有限公司	12	12
杭州安恒信息技术股份有限公司	5	5
远江盛邦（北京）网络安全科技股份有限公司	2	2
江苏云天网络安全技术有限公司	6	6
北京时代新威信息技术有限公司	4	4
北京山石网科信息技术有限公司	3	3
山东正中信息技术股份有限公司	2	2
贵州多彩网安科技有限公司	1	1
北京远禾科技有限公司	1	1
北京天下信安技术有限公司	1	1
CNCERT 河南分中心	1	1
个人	162	162
报送总计	25279	22622

本周漏洞按类型和厂商统计

本周，CNVD 收录了 247 个漏洞。WEB 应用 139 个，应用程序 65 个，网络设备（交换机、路由器等网络端设备）31 个，操作系统 4 个，智能设备（物联网终端设备）3 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	139

应用程序	65
网络设备（交换机、路由器等网络端设备）	31
操作系统	4
智能设备（物联网终端设备）	3
数据库	3
安全产品	2

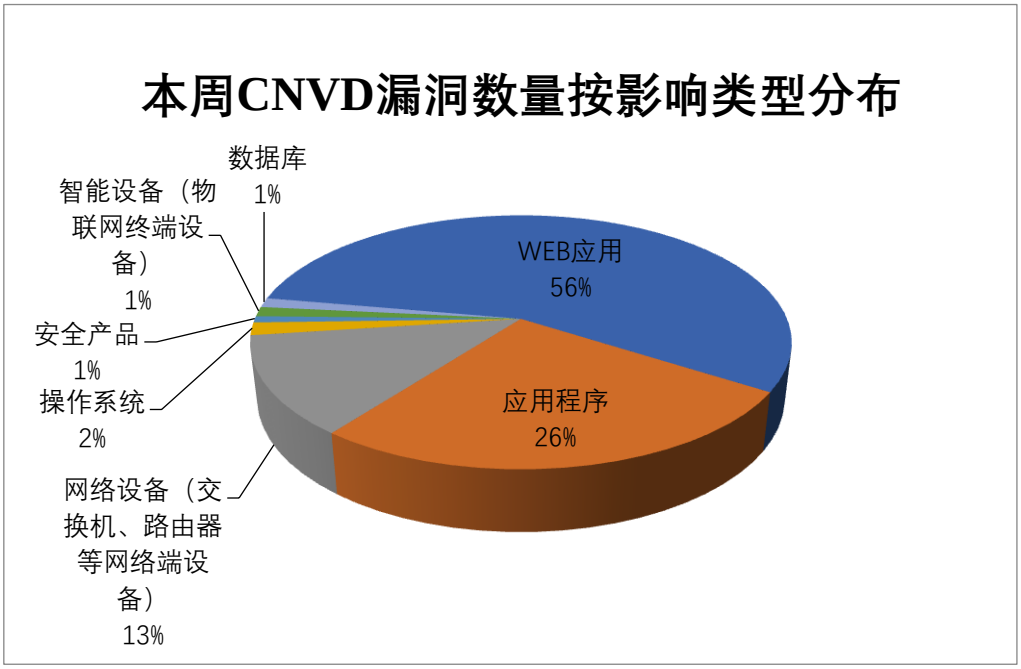

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及用友网络科技股份有限公司、SAP、Google 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	用友网络科技股份有限公司	16	6%
2	SAP	13	5%
3	Google	12	5%
4	Adobe	10	4%
5	DELL	9	4%
6	青岛海信网络科技股份有限公司	9	4%
7	安科瑞电气股份有限公司	7	3%
8	深圳市蓝凌软件股份有限公司	7	3%
9	深圳市吉祥腾达科技有限公司	6	2%

10	其他	158	64%

本周行业漏洞收录情况

本周，CNVD 收录了 16 个电信行业漏洞，3 个移动互联网行业漏洞，2 个工控行业漏洞（如下图所示）。其中，“Rockwell Automation FactoryTalk Services Platform 授权问题漏洞、Rockwell Automation PanelView Plus 代码问题漏洞”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/

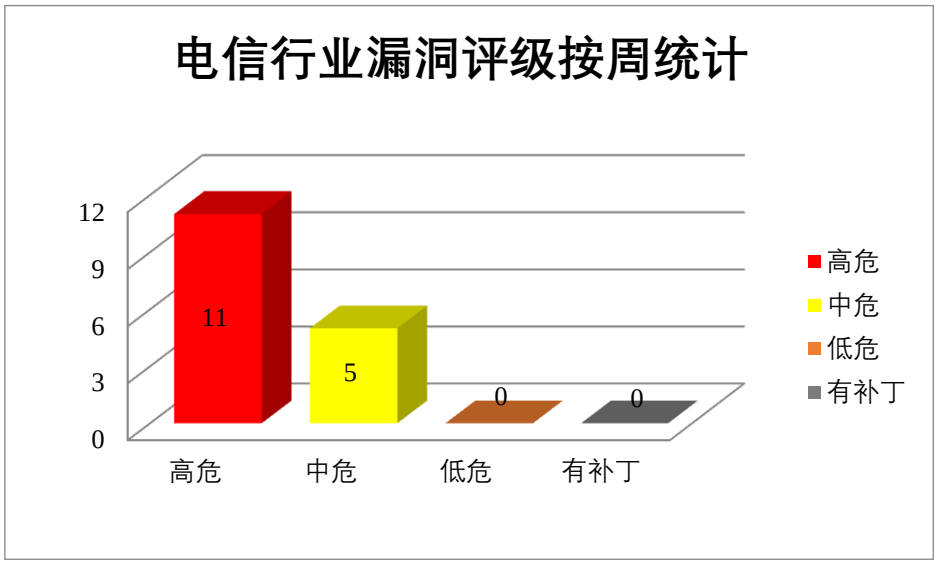

图 3 电信行业漏洞统计

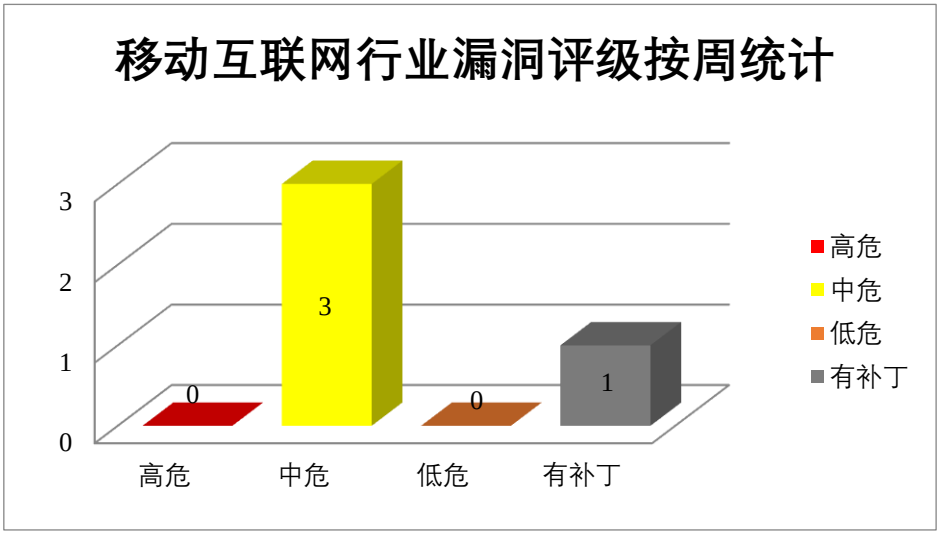

图 4 移动互联网行业漏洞统计

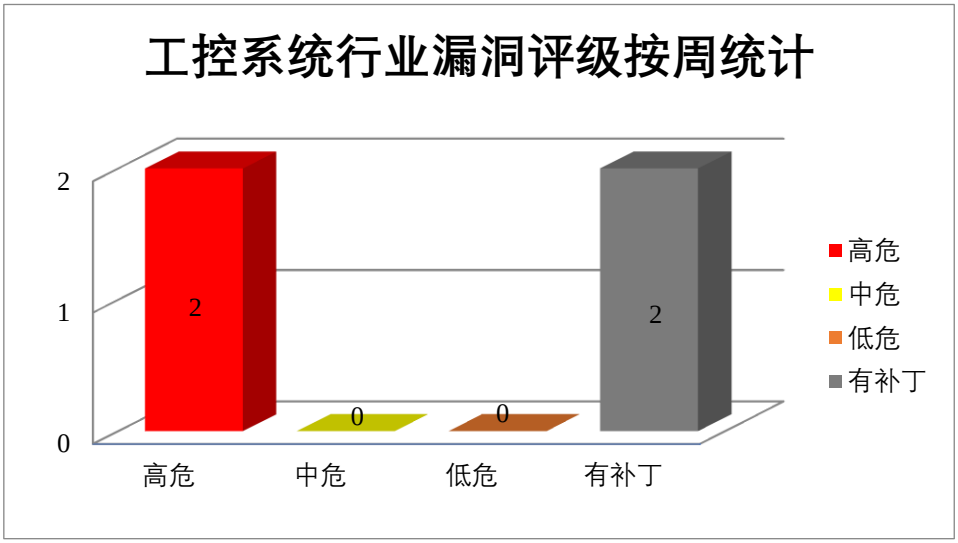

图 5 工控系统行业漏洞统计

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、 Google 产品安全漏洞

Google Chrome 是美国谷歌（Google）公司的一款 Web 浏览器。V8 是其中的一套开源 JavaScript 引擎。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限制，在系统上运行任意代码等。

CNVD 收录的相关漏洞包括：Google Chrome 代码执行漏洞（CNVD-2025-00207、CNVD-2025-00208、CNVD-2025-00209、CNVD-2025-00210、CNVD-2025-00213、CNVD-2025-00214）、Google Chrome 安全绕过漏洞（CNVD-2025-00211、CNVD-2025-00212）。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-2025-00207

https://www.cnvd.org.cn/flaw/show/CNVD-2025-00208

https://www.cnvd.org.cn/flaw/show/CNVD-2025-00209

https://www.cnvd.org.cn/flaw/show/CNVD-2025-00210

https://www.cnvd.org.cn/flaw/show/CNVD-2025-00211

https://www.cnvd.org.cn/flaw/show/CNVD-2025-00212

https://www.cnvd.org.cn/flaw/show/CNVD-2025-00213

https://www.cnvd.org.cn/flaw/show/CNVD-2025-00214

2、 Adobe 产品安全漏洞

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敏感内存泄露，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 Substance 3D Painter 堆缓冲区溢出漏洞（CNVD-2025-00197、CNVD-2025-00200、CNVD-2025-00199）、Adobe Substance 3D Painter 越界读取漏洞（CNVD-2025-00203）、Adobe Substance 3D Painter 越界写入漏洞（CNVD-2025-00205、CNVD-2025-00204、CNVD-2025-00206、CNVD-2025-00198）。其中，除“Adobe Substance 3D Painter 越界读取漏洞（CNVD-2025-00203）”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-2025-00198

https://www.cnvd.org.cn/flaw/show/CNVD-2025-00197

https://www.cnvd.org.cn/flaw/show/CNVD-2025-00200

https://www.cnvd.org.cn/flaw/show/CNVD-2025-00199

https://www.cnvd.org.cn/flaw/show/CNVD-2025-00203

https://www.cnvd.org.cn/flaw/show/CNVD-2025-00205

https://www.cnvd.org.cn/flaw/show/CNVD-2025-00204

https://www.cnvd.org.cn/flaw/show/CNVD-2025-00206

3、DELL 产品安全漏洞

Dell ThinOS 是美国戴尔（Dell）公司的一个客户端操作系统。Dell OpenManage Server Administrator（Dell OMSA）是美国戴尔（Dell）公司的一种软件代理。以两种方式提供全面的一对一系统管理解决方案。Dell RecoverPoint for Virtual Machines 是一款用于虚拟机环境的数据保护和恢复解决方案。Dell NetWorker Management Console 是美国戴尔（Dell）公司的一款备份和恢复软件。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未经授权的权限提升，以 root 身份运行任意命令，从而获得 root 级别的访问权限并可能导致系统完全被攻陷，导致任意命令执行等。

CNVD 收录的相关漏洞包括：Dell ThinOS 命令注入漏洞（CNVD-2024-49615）、Dell OpenManage Server Administrator 授权问题漏洞、Dell RecoverPoint for Virtual Machines OS 命令注入漏洞、Dell RecoverPoint for Virtual Machines 加密问题漏洞、Dell RecoverPoint for Virtual Machines 访问控制错误漏洞、Dell RecoverPoint for Virtual Machines 命令注入漏洞、Dell NetWorker Management Console 信任管理问题漏洞、Dell OpenManage Server Administrator 输入验证错误漏洞。其中，“Dell ThinOS 命令注入漏洞（CNVD-2024-49615）、Dell RecoverPoint for Virtual Machines OS 命令注入漏洞、Dell NetWorker Management Console 信任管理问题漏洞”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-2024-49615

https://www.cnvd.org.cn/flaw/show/CNVD-2024-49621

https://www.cnvd.org.cn/flaw/show/CNVD-2024-49620

https://www.cnvd.org.cn/flaw/show/CNVD-2024-49619

https://www.cnvd.org.cn/flaw/show/CNVD-2024-49618

https://www.cnvd.org.cn/flaw/show/CNVD-2024-49617

https://www.cnvd.org.cn/flaw/show/CNVD-2024-49623

https://www.cnvd.org.cn/flaw/show/CNVD-2024-49622

4、SAP 产品安全漏洞

SAP NetWeaver Administrator（SAP NWA）是德国思爱普（SAP）公司的一个基于 Web 的框架工具，用于管理、配置和监控。SAP HCM Approve Timesheets 是德国思爱普（SAP）公司的一款交易应用软件。SAP NetWeaver Application Server 是德国思爱普（SAP）公司的一款应用程序服务器。SAP Commerce Backoffice 是一个用于管理和维护电子商务网站的强大工具，允许管理员和运营团队轻松地管理网站内容和配置。SAP Commerce Cloud 的 Backoffice 是一个用户中心的、可扩展的后端界面，它允许业务用户轻松管理 SAP Commerce Cloud 中的任何类型的数据。SAP Student Life Cycle Management 是德国思爱普（SAP）公司的一个学生生命周期管理系统。SAP NetWeaver Enterprise Portal 是德国思爱普（SAP）公司的一个 SAP NetWeaver 的 Web 前端组件。SAP NetWeaver AS 是德国思爱普（SAP）公司的一款 SAP 网络应用服务器。它不仅能提供网络服务，且还是 SAP 软件的基本平台。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞探测服务器内网资源，注入恶意脚本或 HTML 代码，当恶意数据被查看时，可获取敏感信息或劫持用户会话，导致特权升级等。

CNVD 收录的相关漏洞包括：SAP NetWeaver Administrator 服务端请求伪造漏洞、SAP HCM Approve Timesheets 授权问题漏洞、SAP NetWeaver Application Server 跨站脚本漏洞（CNVD-2024-49629）、SAP Commerce Backoffice 跨站脚本漏洞、SAP NetWeaver Enterprise Portal 跨站脚本漏洞（CNVD-2024-49627）、SAP Student Life Cycle Management 授权问题漏洞、SAP NetWeaver Enterprise Portal 跨站脚本漏洞（CNVD-2024-49631）、SAP NetWeaver AS 跨站脚本漏洞（CNVD-2024-49630）。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-2024-49625

https://www.cnvd.org.cn/flaw/show/CNVD-2024-49624

https://www.cnvd.org.cn/flaw/show/CNVD-2024-49629

https://www.cnvd.org.cn/flaw/show/CNVD-2024-49628

https://www.cnvd.org.cn/flaw/show/CNVD-2024-49627

https://www.cnvd.org.cn/flaw/show/CNVD-2024-49633

https://www.cnvd.org.cn/flaw/show/CNVD-2024-49631

https://www.cnvd.org.cn/flaw/show/CNVD-2024-49630

5、TP-LINK VN020 缓冲区溢出漏洞

TP-LINK VN020 是中国普联（TP-LINK）公司的一款无线调制解调器。本周，TP-LINK VN020 被披露存在缓冲区溢出漏洞，攻击者可利用该漏洞执行任意代码。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-2024-49642

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-2024-49614	Dell Avamar SQL 注入漏洞（CNVD-2024-49614）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.dell.com/support/kbdoc/en-us/000258636/dsa-2024-489-security-update-for-dell-avamar-and-dell-avamar-virtual-edition-security-update-for-multiple-vulnerabilities
CNVD-2024-49637	Fortinet FortiManager 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：https://docs.fortinet.com/product/fortimanager/7.6
CNVD-2024-49639	Discourse 跨站脚本漏洞（CNVD-2024-49639）	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：https://github.com/discourse/discourse/security/advisories/GHSA-m3v4-v2rp-hfm9
CNVD-2024-49638	Fortinet FortiWLM 路径遍历漏洞（CNVD-2024-49638）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://docs.fortinet.com/document/fortiwlm/8.6.6/release-notes/682570/about-fortiwlm-8-6-6
CNVD-2024-49648	Fortinet FortiOS 访问控制错误漏洞（CNVD-2024-49648）	高	厂商已提供漏洞修补方案，请关注厂商主页及时更新：https://fortiguard.fortinet.com/psirt/FG-IR-23-475
CNVD-2025-00304	Rockwell Automation PanelView Plus 代码问题漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1

			140724
CNVD-2025-00303	Rockwell Automation FactoryTalk Services Platform 授权问题漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://rockwellautomation.custhelp.com/app/answers/answer_view/a_id/1085012/loc/en_US#__highlight
CNVD-2025-00215	Google Chrome 安全绕过漏洞（CNVD-2025-00215）	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：https://issues.chromium.org/issues/42270190
CNVD-2025-00216	Google Chrome 安全绕过漏洞（CNVD-2025-00216）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://chromereleases.googleblog.com/2024/09/stable-channel-update-for-desktop_17.html
CNVD-2025-00201	Adobe Substance 3D Painter 不受信任搜索路径漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://helpx.adobe.com/security/products/substance3d_painter/apsb24-86.html

小结：本周，Google 产品被披露存在多个漏洞，攻击者可利用漏洞在系统上执行任意代码，导致敏感内存泄露等。此外，Adobe、DELL、SAP 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限制，导致敏感内存泄露，在当前用户的上下文中执行任意代码等。另外，TP-LINK VN020 被披露存在缓冲区溢出漏洞，攻击者可利用该漏洞执行任意代码。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、 JFinalCMS 跨站请求伪造漏洞（CNVD-2024-49644）

验证描述

JFinalCMS 是一个内容管理系统。

JFinalCMS 1.0 版本存在跨站请求伪造漏洞，该漏洞源于/admin/tag/save 文件未充分验证请求是否来自可信用户。攻击者可利用该漏洞伪造恶意请求诱骗受害者点击执行敏感操作。

验证信息

POC 链接：https://github.com/hadagaga/vuln/blob/master/JFinalCMS/Cross_Site_Request_Forgery/Cross-Site-Request-Forgery.md

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2024-49644

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. 华硕路由器漏洞允许任意代码执行

华硕公司在某些固件系列中发现了注入和执行漏洞，这些漏洞可能允许经过身份验证的攻击者通过华硕路由器的 AiCloud 功能触发命令执行。

参考链接：https://cybersecuritynews.com/asus-router-vulnerabilities/

2. 已打补丁但仍有漏洞，Windows BitLocker 加密再次被绕过

该漏洞允许攻击者绕过 BitLocker 加密并访问敏感数据，即使是在据称已针对该漏洞打了补丁的系统上也是如此 。

参考链接：https://www.anquanke.com/post/id/303246

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