国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2024 年 09 月 02 日-2024 年 09 月 08 日 **2024 年第 36 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 322 个，其中高危漏洞 177 个、中危漏洞 129 个、低危漏洞 16 个。漏洞平均分值为 6.96。本周收录的漏洞中，涉及 0day 漏洞 195 个（占 61%），其中互联网上出现“SeaCMS 代码执行漏洞（CNVD-2024-37605）、 FastCMS 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 7902 个，与上周（33921 个）环比减少 77%。

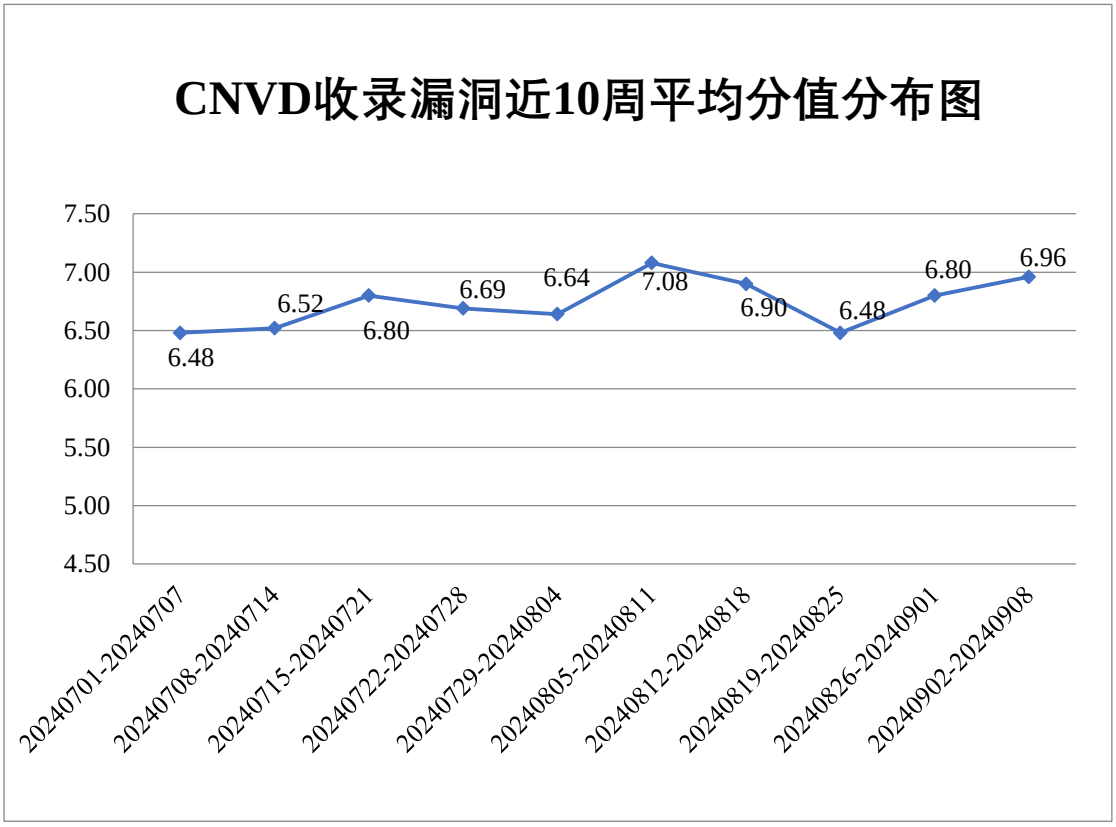

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 2 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 463 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 36 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 6 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：

紫光软件系统有限公司、紫光股份有限公司、重庆森鑫炬科技有限公司、智互联（深圳）科技有限公司、浙江宇视科技有限公司、浙江齐治科技股份有限公司、浙江大华技术股份有限公司、友讯电子设备（上海）有限公司、用友网络科技股份有限公司、夏普科技（上海）有限公司、网是科技股份有限公司、天津神舟通用数据技术有限公司、搜狗公司、世邦通信股份有限公司、神州数码控股有限公司、深圳市思迅软件股份有限公司、深圳市吉祥腾达科技有限公司、深圳市必联电子有限公司、深圳勤杰软件有限公司、深电能科技集团有限公司、上海甄云信息科技有限公司、上海居亦科技发展有限公司、上海建业信息科技股份有限公司、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、山东比特智能科技股份有限公司、润申标准化技术服务（上海）有限公司、瑞斯康达科技发展股份有限公司、青岛海信网络科技股份有限公司、青岛东胜伟业软件科技有限公司、品茗科技股份有限公司、迈普通信技术股份有限公司、柯尼卡美能达集团、敬业钢铁有限公司、江苏群杰物联科技有限公司、坚力世纪国际软件（北京）有限公司、佳能（中国）有限公司、济源市大洋网络科技有限公司、惠普贸易（上海）有限公司、河南觅云仓信息科技有限公司、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、杭州新中大科技股份有限公司、杭州三汇信息工程有限公司、杭州品联科技有限公司、杭州科强信息技术有限公司、杭州吉拉科技有限公司、杭州海康威视数字技术股份有限公司、哈尔滨新中新电子股份有限公司、国电南瑞科技股份有限公司、广州万户网络技术有限公司、广州市保伦电子有限公司、广西金中软件集团有限公司、广东飞讯工业互联网有限公司、方天科技（深圳）有限公司、东莞市同享软件科技有限公司、大连爱智控制系统有限公司、创业慧康科技股份有限公司、畅捷通信息技术股份有限公司、北京中犇科技有限公司、北京亿赛通科技发展有限责任公司、北京星网锐捷网络技术有限公司、北京西斯耐特自动化技术有限公司、北京万户网络技术有限公司、北京通达志成科技有限公司、北京神州视翰科技有限公司、北京南琼电子有限责任公司、北京美特软件技术有限公司、北京金和网络股份有限公司、北京国信创新科技股份有限公司、北京北大方正电子有限公司、北京奥博威斯科技有限公司、北京傲盾软件有限责任公司、奥琦玮信息科技（北京）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、安徽海软信息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，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、北京天融信网络安全技术有限公司、阿里云计算有限公司等单位报送公开收集的漏洞数量较多。成都卫士通信息安全技术有限公司、河南东方云盾信息技术有限公司、重庆都会信息科技、江苏正信信息安全测试有限公司、江苏云天网络安全技术有限公司、北京翰慧投资咨询有限公司、上海观安信息技术股份有限公司及其他个人白帽子向 CNVD 提交了 7902 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）、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 7586 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）	6570	6570
三六零数字安全科技集团有限公司	790	790
北京神州绿盟科技有限公司	578	0
深信服科技股份有限公司	506	1
安天科技集团股份有限公司	453	0
北京天融信网络安全技术有限公司	282	0
上海交大	226	226
阿里云计算有限公司	174	0
京东科技信息技术有限公司	114	0
北京数字观星科技有限公司	83	0
恒安嘉新（北京）科技股份公司	82	0
北京启明星辰信息安全技术有限公司	68	0

北京长亭科技有限公司	34	0
杭州安恒信息技术股份有限公司	33	13
中国电信集团系统集成有限责任公司	25	3
北京知道创宇信息技术有限公司	23	0
快页信息技术有限公司	9	9
北京安信天行科技有限公司	7	7
北京智游网安科技有限公司	1	1
杭州迪普科技股份有限公司	1	1
成都卫士通信息安全技术有限公司	25	25
河南东方云盾信息技术有限公司	7	7
重庆都会信息科技	4	4
江苏正信信息安全测试有限公司	2	2
江苏云天网络安全技术有限公司	1	1
北京翰慧投资咨询有限公司	1	1
上海观安信息技术股份有限公司	1	1
CNCERT 河北分中心	3	3
个人	237	237
报送总计	10340	7902

本周漏洞按类型和厂商统计

本周，CNVD 收录了 322 个漏洞。WEB 应用 176 个，应用程序 116 个，网络设备（交换机、路由器等网络端设备）17 个，操作系统 7 个，智能设备（物联网终端设备）4 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	176
应用程序	116
网络设备（交换机、路由器等网络端设备）	17
操作系统	7
智能设备（物联网终端设备）	4
安全产品	2

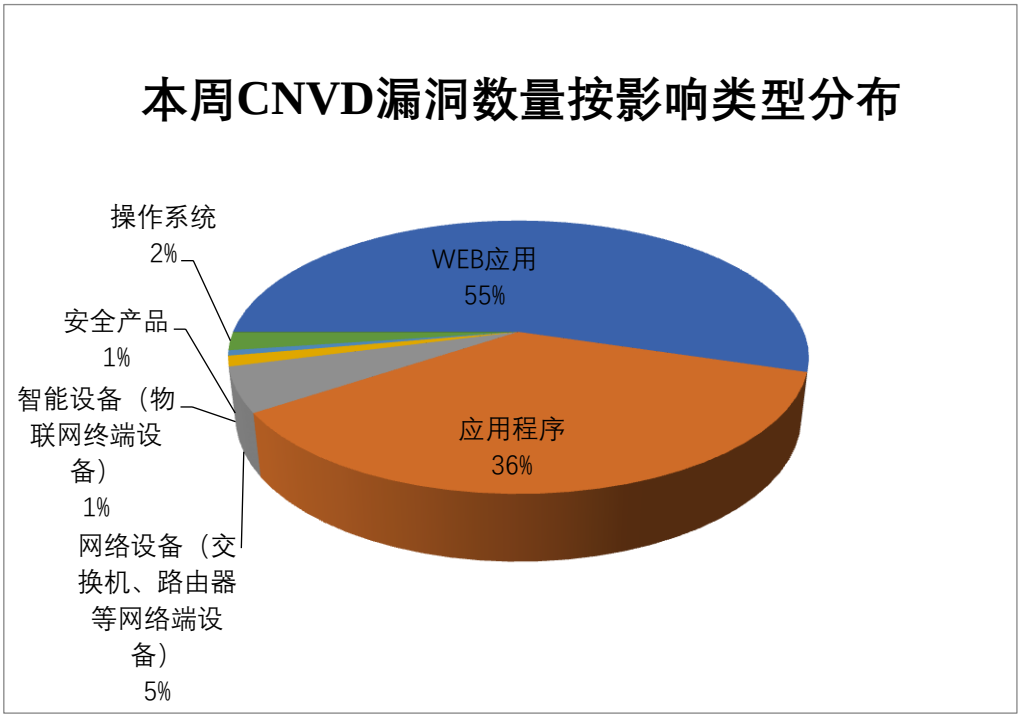

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Kashipara、NetBox、SWFTools 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	Kashipara	26	8%
2	NetBox	18	6%
3	SWFTools	16	5%
4	Kliqqi	16	5%
5	用友网络科技股份有限公司	15	4%

6	Mozilla	12	4%
7	DELL	11	4%
8	Zoho	11	3%
9	GTKWave	10	3%
10	其他	187	58%

本周行业漏洞收录情况

本周，CNVD 收录了 10 个电信行业漏洞，4 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，“Cisco Small Business 缓冲区溢出漏洞（CNVD-2024-37606）、Rockwell Automation FactoryTalk View SE 输入验证错误漏洞（CNVD-2024-37628）”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/

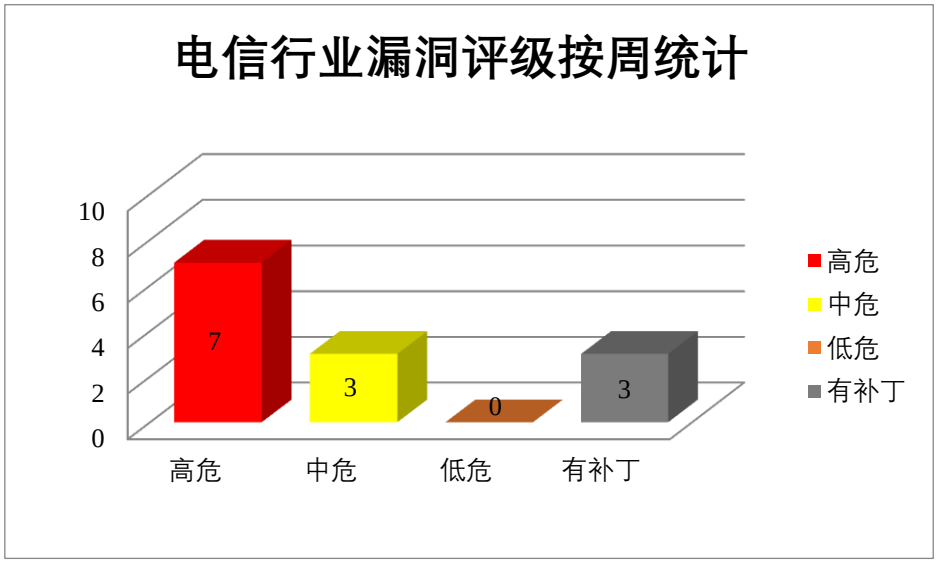

图 3 电信行业漏洞统计

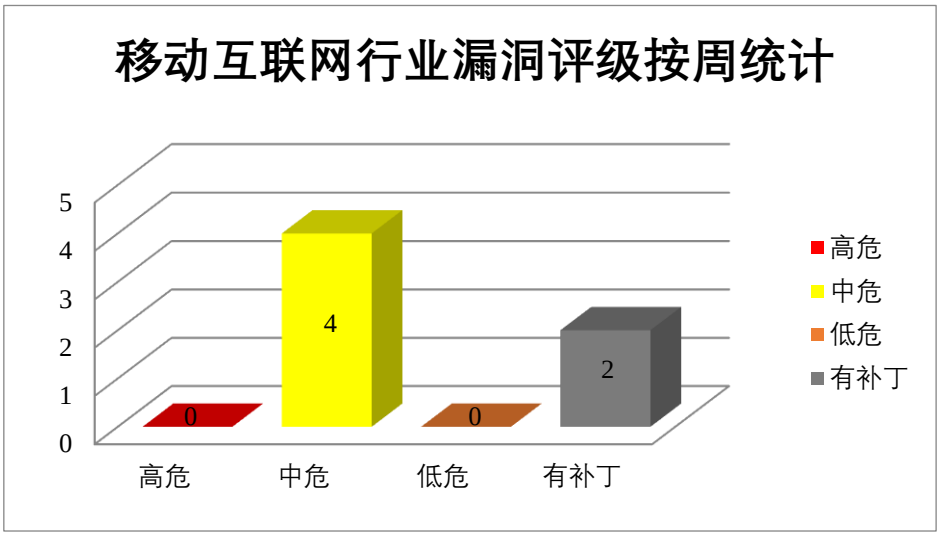

图 4 移动互联网行业漏洞统计

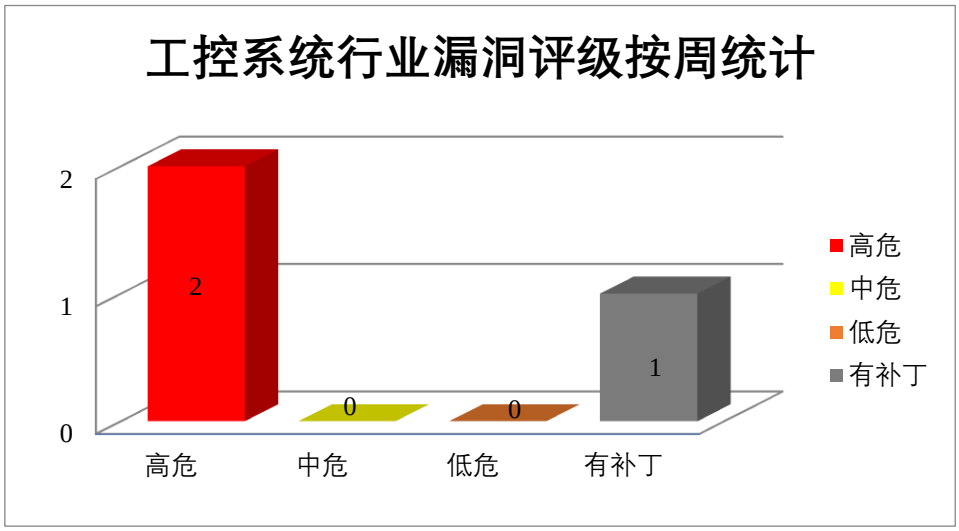

图 5 工控系统行业漏洞统计

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、IBM 产品安全漏洞

IBM InfoSphere Information Server 是美国国际商业机器（IBM）公司的一套数据整合平台。该平台可用于整合各种渠道获取的数据信息。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 URL 信息中返回的敏感信息，消耗文件空间资源，在 Web UI 中嵌入任意 JavaScript 代码，导致可信会话中的凭据泄露等。

CNVD 收录的相关漏洞包括：IBM InfoSphere Information Server 信息泄露漏洞（CNVD-2024-37060、CNVD-2024-37059、CNVD-2024-37063）、IBM InfoSphere Information Server 拒绝服务漏洞（CNVD-2024-37058）、IBM InfoSphere Information Server 服务器端请求伪造漏洞、IBM InfoSphere Information Server 跨站脚本漏洞（CNVD-20

24-37062、CNVD-2024-37061、CNVD-2024-37065）。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-2024-37060
https://www.cnvd.org.cn/flaw/show/CNVD-2024-37059
https://www.cnvd.org.cn/flaw/show/CNVD-2024-37058
https://www.cnvd.org.cn/flaw/show/CNVD-2024-37064
https://www.cnvd.org.cn/flaw/show/CNVD-2024-37063
https://www.cnvd.org.cn/flaw/show/CNVD-2024-37062
https://www.cnvd.org.cn/flaw/show/CNVD-2024-37061
https://www.cnvd.org.cn/flaw/show/CNVD-2024-37065

2、 Mozilla 产品安全漏洞

Mozilla Firefox 是一款开源 Web 浏览器。Mozilla Firefox ESR 是 Firefox（Web 浏览器）的一个延长支持版本。Mozilla Thunderbird 是一套从 Mozilla Application Suite 独立出来的电子邮件客户端软件。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞绕过安全限制，导致越界读取，在系统上执行任意代码或造成拒绝服务等。

CNVD 收录的相关漏洞包括：多款 Mozilla 产品拒绝服务漏洞（CNVD-2024-37197）、Mozilla Firefox 和 Firefox ESR 信息泄露漏洞（CNVD-2024-37122）、Mozilla Firefox 代码执行漏洞（CNVD-2024-37191、CNVD-2024-37195）、多款 Mozilla 产品代码执行漏洞（CNVD-2024-37196、CNVD-2024-37198、CNVD-2024-37190）、多款 Mozilla 产品安全绕过漏洞（CNVD-2024-37199）。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-2024-37122
https://www.cnvd.org.cn/flaw/show/CNVD-2024-37190
https://www.cnvd.org.cn/flaw/show/CNVD-2024-37191
https://www.cnvd.org.cn/flaw/show/CNVD-2024-37195
https://www.cnvd.org.cn/flaw/show/CNVD-2024-37196
https://www.cnvd.org.cn/flaw/show/CNVD-2024-37197
https://www.cnvd.org.cn/flaw/show/CNVD-2024-37198
https://www.cnvd.org.cn/flaw/show/CNVD-2024-37199

3、 Fortinet 产品安全漏洞

Fortinet FortiWebManager 是美国飞塔（Fortinet）公司的一款 Web 应用防火墙。Fortinet FortiExtender 是美国飞塔（Fortinet）公司的一款无线 WAN（广域网）扩展器设备。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 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 FortiWAN 是美国飞塔（Fortinet）公司的一个用于在不同网络之间执行负载平衡和容错的网络设备。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。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 HTTP 请求或 CLI 执行未经授权的代码或命令，通过精心设计的 HTTP 请求创建具有提升权限的用户，提交特殊的请求，可以应用程序上下文执行任意命令等。

CNVD 收录的相关漏洞包括：Fortinet FortiWebManager 授权问题漏洞、Fortinet FortiExtender 访问控制错误漏洞（CNVD-2024-37340）、Fortinet FortiOS 访问控制错误漏洞（CNVD-2024-37339）、Fortinet FortiNAC 授权问题漏洞（CNVD-2024-37344）、Fortinet FortiNAC 存在反序列化漏洞、Fortinet FortiWAN 操作系统命令注入漏洞（CNVD-2024-37348）、Fortinet FortiPortal 信息泄露漏洞、Fortinet FortiExtender 命令注入漏洞（CNVD-2024-37345）。其中，“Fortinet FortiExtender 访问控制错误漏洞（CNVD-2024-37340）、Fortinet FortiNAC 存在反序列化漏洞、Fortinet FortiWAN 操作系统命令注入漏洞（CNVD-2024-37348）、Fortinet FortiExtender 命令注入漏洞（CNVD-2024-37345）”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-2024-37341

https://www.cnvd.org.cn/flaw/show/CNVD-2024-37340

https://www.cnvd.org.cn/flaw/show/CNVD-2024-37339

https://www.cnvd.org.cn/flaw/show/CNVD-2024-37344

https://www.cnvd.org.cn/flaw/show/CNVD-2024-37342

https://www.cnvd.org.cn/flaw/show/CNVD-2024-37348

https://www.cnvd.org.cn/flaw/show/CNVD-2024-37347

https://www.cnvd.org.cn/flaw/show/CNVD-2024-37345

4、DELL 产品安全漏洞

Dell Alienware Command Center 是美国戴尔（Dell）公司的一个软件包管理器。Dell Data Lakehouse 是美国戴尔（Dell）公司的一个完全集成的数据平台。Dell BIOS 是美国戴尔（Dell）公司的一个计算机主板上小型内存芯片上的嵌入式软件。Dell Power Manager 是美国戴尔（Dell）公司的一款应用程序，用于配置电池维护方式，从而更大限度地提高系统的电池续航时间。Dell PowerScale OneFS 是美国戴尔（Dell）公司的一个操作系统。提供横向扩展 NAS 的 PowerScale OneFS 操作系统。Dell Edge Gateway 是美国戴尔（Dell）公司的一系列智能网关设备。旨在聚合、保护、分析和中继来自网络边缘各种传感器和设备的数据。Dell EMC Repository Manager 是美国戴尔（Dell）

公司的 Dell OpenManage 产品组合内一款可以让 IT 管理员轻松管理系统更新的应用程序。Dell Repository Manager 提供了可搜索的界面，用于创建自定义软件集合，这些集合被称为 Dell Update Package (DUP)的捆绑包和存储库。Dell OS Recovery Tool 是美国戴尔（Dell）公司的一个操作系统恢复工具。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信息泄露，进行代码执行和权限提升等。

CNVD 收录的相关漏洞包括：Dell Alienware Command Center 访问控制错误漏洞（CNVD-2024-37422）、Dell Data Lakehouse 加密问题漏洞、Dell BIOS 输入验证错误漏洞（CNVD-2024-37419）、Dell Power Manager 授权问题漏洞、Dell PowerScale OneFS 加密问题漏洞（CNVD-2024-37424）、Dell Edge Gateway 缓冲区溢出漏洞（CNVD-2024-37423）、Dell EMC Repository Manager 访问控制错误漏洞、Dell OS Recovery Tool 访问控制错误漏洞（CNVD-2024-3742694）。其中，“Dell PowerScale OneFS 加密问题漏洞（CNVD-2024-37424）”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-2024-37422
https://www.cnvd.org.cn/flaw/show/CNVD-2024-37421
https://www.cnvd.org.cn/flaw/show/CNVD-2024-37419
https://www.cnvd.org.cn/flaw/show/CNVD-2024-37418
https://www.cnvd.org.cn/flaw/show/CNVD-2024-37424
https://www.cnvd.org.cn/flaw/show/CNVD-2024-37423
https://www.cnvd.org.cn/flaw/show/CNVD-2024-37427
https://www.cnvd.org.cn/flaw/show/CNVD-2024-37426

5、Fortinet FortiNAC 授权问题漏洞（CNVD-2024-37343）

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。本周，Fortinet FortiNAC 被披露存在授权问题漏洞。攻击者可利用该漏洞通过客户端安全重新协商对设备执行 DoS 攻击。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-2024-37343

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-2024-37200	GTKWave 代码执行漏洞（CNVD-2024-37200）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://sourceforge.net/projects/gtkwa

			ve/files/gtkwave-3.3.118/
CNVD-2024-37201	GTKWave 缓冲区溢出漏洞（CNVD-2024-37201）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://sourceforge.net/projects/gtkwave/files/gtkwave-3.3.118/
CNVD-2024-37502	Microsoft Edge (Chromium-based)远程代码执行漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-38210
CNVD-2024-37480	ZOHO ManageEngine ADAudit Plus SQL 注入漏洞（CNVD-2024-37480）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.manageengine.com/products/active-directory-audit/cve-2024-5556.html
CNVD-2024-37606	Cisco Small Business 缓冲区溢出漏洞（CNVD-2024-37606）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-multi-85G83CRB
CNVD-2024-37470	SWFTools bufferWriteData 方法内存错误引用漏洞	高	厂商已提供漏洞修复方案，请关注厂商主页更新：https://github.com/matthiaskramm/swftools/issues/211
CNVD-2024-37492	Microsoft Exchange Server 欺骗漏洞（CNVD-2024-37492）	高	目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载：https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36039
CNVD-2024-37473	SWFTools q.c 页面缓冲区溢出漏洞	高	目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载：https://github.com/matthiaskramm/swftools/issues/210
CNVD-2024-37476	SWFTools swfc.c:2576 页面缓冲区溢出漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/matthiaskramm/swftools/issues/207
CNVD-2024-37477	SWFTools swfc.c:2587 页面缓冲区溢出漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/matthiaskramm/swftools/issues/209

小结：本周，IBM 产品被披露存在多个漏洞，攻击者可利用漏洞获取 URL 信息中

返回的敏感信息，消耗文件空间资源，在 Web UI 中嵌入任意 JavaScript 代码，导致可信会话中的凭据泄露等。此外，Mozilla、Fortinet、DELL 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，导致越界读取，在系统上执行任意代码或造成拒绝服务等。另外，Fortinet FortiNAC 被披露存在授权问题漏洞。攻击者可利用该漏洞通过客户端安全重新协商对设备执行 DoS 攻击。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、SeaCMS 代码执行漏洞（CNVD-2024-37605）

验证描述

SeaCMS 是海洋 CMS（SeaCMS）公司的一套使用 PHP 编写的免费、开源的网站内容管理系统。该系统主要被设计用来管理视频点播资源。

SeaCMS 13.0 版本存在代码执行漏洞，该漏洞源于 admin_editplayer.php 对文件的编辑限制可以被绕过，攻击者可利用该漏洞导致任意代码执行。

验证信息

POC 链接：https://gitee.com/fushuling/cve/blob/master/SeaCMS%20V13%20admin_editplayer.php%20code%20injection.md

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2024-37605

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. Apache 修复了关键的 OFBiz 远程代码执行漏洞

Apache 已修复其开源 OFBiz（Open For Business） 软件中的一个严重安全漏洞，该漏洞可能允许攻击者在易受攻击的 Linux 和 Windows 服务器上执行任意代码。

参考链接：https://www.bleepingcomputer.com/news/security/apache-fixes-critical-ofbiz-remote-code-execution-vulnerability/

2. LiteSpeed 曝出严重漏洞，致使超 600 万 WordPress 网站遭攻击

近日，Patchstack 的 Rafie Muhammad 在 LiteSpeed Cache 插件中发现了一个严重漏

洞，该插件主要用于加快超 600 万个 WordPress 网站的用户浏览速度。

参考链接：https://www.bleepingcomputer.com/news/security/litespeed-cache-bug-exposes-6-million-wordpress-sites-to-takeover-attacks/

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