国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2022 年 10 月 31 日-2022 年 11 月 06 日 **2022 年第 44 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 635 个，其中高危漏洞 298 个、中危漏洞 286 个、低危漏洞 51 个。漏洞平均分值为 6.46。本周收录的漏洞中，涉及 0day 漏洞 538 个（占 85%），其中互联网上出现“fast-string-search 拒绝服务漏洞、Online Project Time Management System 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事件型漏洞总数 16853 个，与上周（13636 个）环比增加 24%。

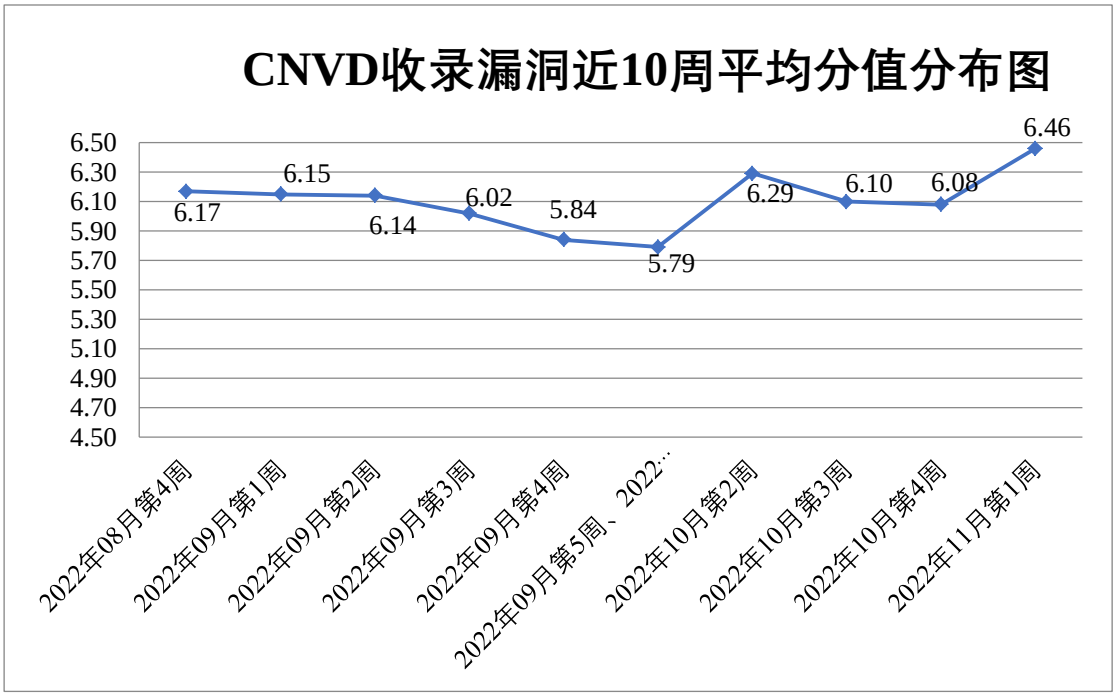

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 23 起，向基础电

信企业通报漏洞事件 25 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 1001 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 283 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 62 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：

珠海玖时光科技有限公司、珠海金山办公软件有限公司、浙江大华技术股份有限公司、用友网络科技股份有限公司、永中软件股份有限公司、阳光电源股份有限公司、兄弟（中国）商业有限公司、信呼、西安瑞友信息技术资讯有限公司、武汉深之度科技有限公司、武汉达梦数据库股份有限公司、潍坊家园驿站电子技术有限公司、统信软件技术有限公司、天维尔信息科技股份有限公司、天地伟业技术有限公司、腾讯安全应急响应中心、台达电子企业管理（上海）有限公司、四川征云网络科技有限公司、四川云时网络科技有限公司、数字广东网络建设有限公司、世邦通信股份有限公司、深圳智沃科技有限公司、深圳搜豹网络有限公司、深圳市亿玛信诺科技有限公司、深圳市网心科技有限公司、深圳市任网游科技发展有限公司、深圳市吉祥腾达科技有限公司、深圳市惠尔顿信息技术有限公司、深圳市河湾科技有限公司、深圳市博思协创网络科技有限公司、深圳锐取信息技术股份有限公司、上海卓卓网络科技有限公司、上海云翌通信科技有限公司、上海好快科技有限公司、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、熵基科技股份有限公司、山东山大华天软件有限公司、山东金田水利科技有限公司、厦门市百胜通软件技术有限公司、厦门快普信息技术有限公司、清枫（北京）科技有限公司、青果软件集团有限公司、青岛易软天创网络科技有限公司、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、麒麟软件有限公司、南宁迈世信息技术有限公司、南昌卓蓝科技有限公司、美图公司、眉山市爱客网络科技有限公司、联奕科技股份有限公司、朗坤智慧科技股份有限公司、金蝶天燕云计算股份有限公司、江西铭软科技有限公司、佳能（中国）有限公司、吉翁电子（深圳）有限公司、华夏 ERP、湖北心拓心理健康科技有限公司、泓华国际医疗控股有限公司、合肥六出网络科技有限公司、杭州雄伟科技开发股份有限公司、杭州赛凡科技有限公司、杭州美迪软件有限公司、杭州可道云网络有限公司、贵州觅新科技有限公司、广州市品高软件股份有限公司、广州宁静海信息科技有限公司、广州极电通信技术有限公司、广州多益网络股份有限公司、广东支付通科技有限公司、福州联讯信息科技有限公司、福建平潭海峡中药材交易有限责任公司、福建创意嘉和软件有限公司、福建博思软件股份有限公司、东莞誉云网络科技有限公司、大唐电信科技股份有限公司、大连华天软件有限公司、成都卓越远扬信息技术有限公司、成都海信达科技有限公司、成都飞鱼星科技股份有限公司、成都傲梅科技有限公司、畅捷通信息技术股份有限公司、北京中远麒麟科技有限公司、北京中科华博科技有限公司、北京致远互联软件股份有限公司、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、北京通达信科科技有限公司、北京联合信任技术服务有限公司、北京力控元通科技有限公司、北京九思协同软件有限公司、北京竞业达数码科技股份有限公司、北京火绒网络科技有限公司、北京国炬信息技术有限公司、北京东方通科技股份有限公司、北京北信源软件股份有限公司、北京佰才邦技术股份有限公司、北京百卓网络技术有限公司、北京奥博威斯科技有限公司、安徽微同科技有限公司、RPCMS、emlog、Elasticsearch、Doccms 和 BEESCMS。

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、北京神州绿盟科技有限公司、安天科技集团股份有限公司、南京众智维信息科技有限公司等单位报送公开收集的漏洞数量较多。贵州泰若数字科技有限公司、北京山石网科信息技术有限公司、北京云科安信科技有限公司（Seraph 安全实验室）、北京升鑫网络科技有限公司、安徽锋刃信息科技有限公司、杭州迪普科技股份有限公司、江苏保旺达软件技术有限公司、奇安星城网络安全运营服务（长沙）有限公司、山东云天安全技术有限公司、河南东方云盾信息技术有限公司、苏州棱镜七彩信息科技有限公司、山东新潮信息技术有限公司、河南信安世纪科技有限公司、河南灵创电子科技有限公司、北京华顺信安信息技术有限公司、中能融合智慧科技有限公司、云南联创网安科技有限公司、苏州众里数码科技有限公司、北京东方通科技股份有限公司、中国电信股份有限公司网络安全产品运营中心、北京微步在线科技有限公司、西安敏恒信息技术有限公司、西安交大捷普网络科技有限公司、任子行网络技术股份有限公司、上海纽盾科技股份有限公司、河南天祺信息安全技术有限公司、杭州默安科技有限公司、联通数字科技有限公司、信息产业信息安全测评中心、江西和尔惠信息技术有限公司、贵州电网有限责任公司信息中心、北京万户网络技术有限公司、张家界市百鸟信安科技有限公司、杭州美创科技有限公司、博智安全科技股份有限公司、快页信息技术有限公司、浙江木链物联网科技有限公司、北京华云安信息技术有限公司、山石网科通信技术股份有限公司及其他个人白帽子向 CNVD 提交了 16853 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）、上海交大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 13889 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）	9094	9094
三六零数字安全科技集团有限公司	1963	1963
奇安信网神（补天平	1649	1649

台）		
上海交大	1183	1183
深信服科技股份有限公司	485	0
新华三技术有限公司	410	0
北京神州绿盟科技有限公司	316	0
安天科技集团股份有限公司	269	0
南京众智维信息科技有限公司	251	251
北京天融信网络安全技术有限公司	210	2
北京数字观星科技有限公司	135	0
西安四叶草信息技术有限公司	121	121
杭州安恒信息技术股份有限公司	104	67
恒安嘉新（北京）科技股份公司	100	0
远江盛邦（北京）网络安全科技股份有限公司	99	99
北京启明星辰信息安全技术有限公司	73	15
浙江大华技术股份有限公司	27	27
中国电信集团系统集成有限责任公司	20	1
京东科技信息技术有限公司	19	19
北京知道创宇信息技术有限公司	15	0
卫士通信息产业股份	7	7

有限公司		
内蒙古云科数据服务股份有限公司	3	3
北京长亭科技有限公司	1	1
深圳市腾讯计算机系统有限公司（玄武实验室）	1	1
贵州泰若数字科技有限公司	342	342
北京山石网科信息技术有限公司	293	293
北京云科安信科技有限公司（Seraph 安全实验室）	192	192
北京升鑫网络科技有限公司	137	137
安徽锋刃信息科技有限公司	24	24
杭州迪普科技股份有限公司	22	8
江苏保旺达软件技术有限公司	14	14
奇安星城网络安全运营服务（长沙）有限公司	12	12
山东云天安全技术有限公司	10	10
河南东方云盾信息技术有限公司	10	10
苏州棱镜七彩信息科技有限公司	9	9
山东新潮信息技术有限公司	7	7
河南信安世纪科技有	6	6

限公司		
河南灵创电子科技有限公司	6	6
北京华顺信安信息技术有限公司	5	5
中能融合智慧科技有限公司	4	4
云南联创网安科技有限公司	4	4
苏州众里数码科技有限公司	3	3
北京东方通科技股份有限公司	3	3
中国电信股份有限公司网络安全产品运营中心	3	3
北京微步在线科技有限公司	2	2
西安敏恒信息技术有限公司	2	2
西安交大捷普网络科技有限公司	2	2
任子行网络技术股份有限公司	2	2
上海纽盾科技股份有限公司	1	1
河南天祺信息安全技术有限公司	1	1
杭州默安科技有限公司	1	1
联通数字科技有限公司	1	1
信息产业信息安全测评中心	1	1
江西和尔惠信息技术	1	1

有限公司		
贵州电网有限责任公司信息中心	1	1
北京万户网络技术有限公司	1	1
张家界市百鸟信安科技有限公司	1	1
杭州美创科技有限公司	1	1
博智安全科技股份有限公司	1	1
快页信息技术有限公司	1	1
浙江木链物联网科技有限公司	1	1
北京华云安信息技术有限公司	1	1
山石网科通信技术股份有限公司	1	1
CNCERT 浙江分中心	9	9
CNCERT 贵州分中心	4	4
CNCERT 内蒙古分中心	2	2
CNCERT 四川分中心	2	2
个人	1218	1218
报送总计	18919	16853

本周漏洞按类型和厂商统计

本周，CNVD 收录了 635 个漏洞。WEB 应用 331 个，应用程序 138 个，网络设备（交换机、路由器等网络端设备）117 个，操作系统 23 个，智能设备（物联网终端设备）20 个，安全产品 6 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	331

应用程序	138
网络设备（交换机、路由器等网络端设备）	117
操作系统	23
智能设备（物联网终端设备）	20
安全产品	6

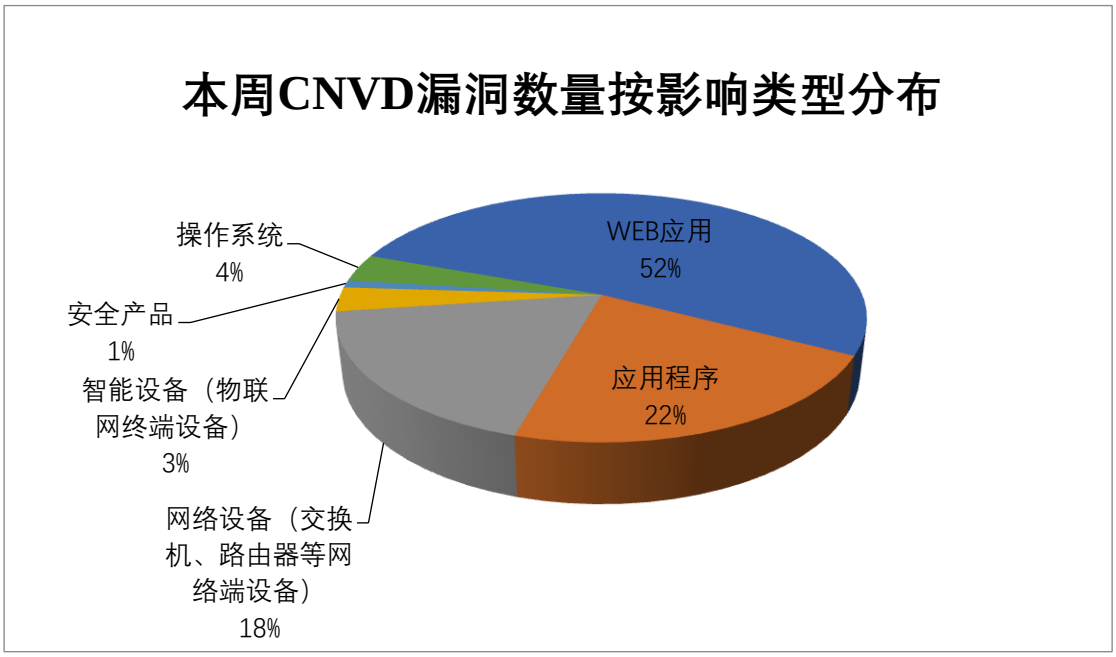

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Apache、新华三技术有限公司、WordPress 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	Apache	21	3%
2	新华三技术有限公司	19	3%
3	WordPress	12	2%
4	深圳市吉祥腾达科技有限公司	11	2%
5	F5	11	2%
6	Linux	10	2%
7	Microsoft	9	1%
8	TOTOLINK	9	1%
9	Telesquare	8	1%
10	其他	525	83%

本周行业漏洞收录情况

本周，CNVD 收录了 94 个电信行业漏洞，36 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，“Google Android 权限许可和访问控制问题漏洞（CNVD-2022-72440）、Apache Tomcat 环境问题漏洞（CNVD-2022-74082）”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/

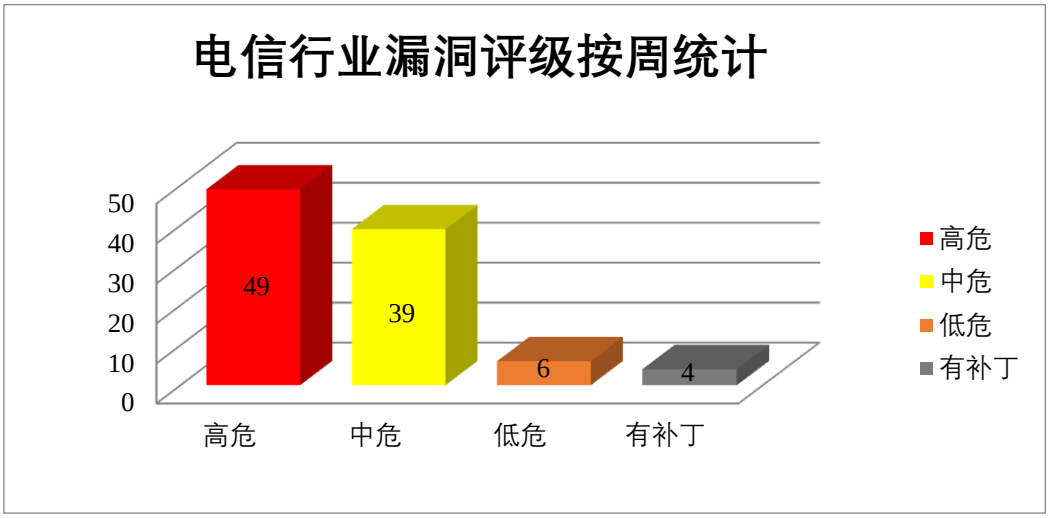

图 3 电信行业漏洞统计

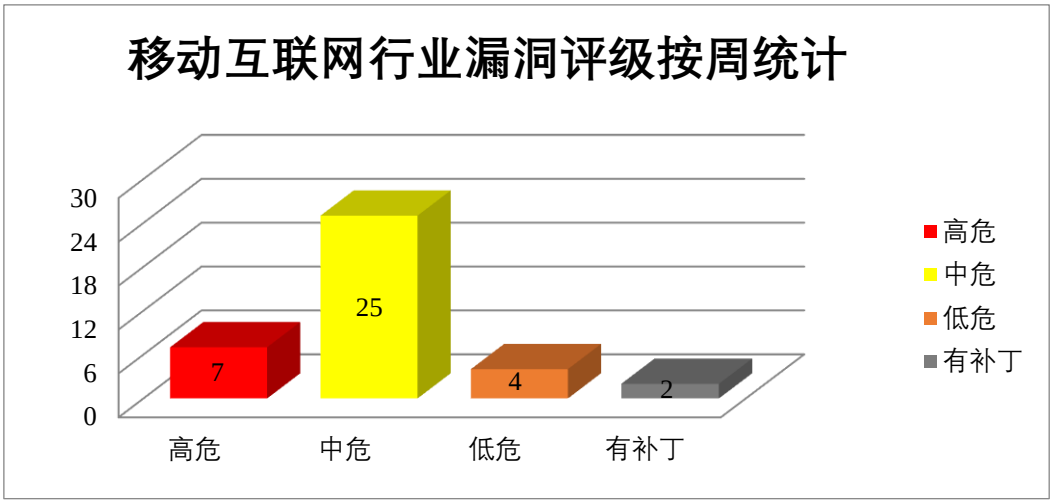

图 4 移动互联网行业漏洞统计

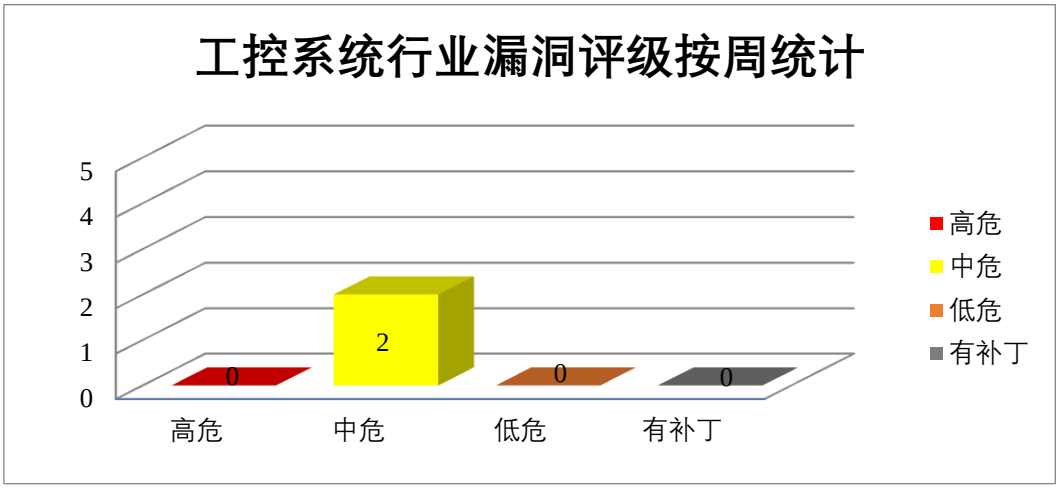

图 5 工控系统行业漏洞统计

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、Linux 产品安全漏洞

Linux kernel 是美国 Linux 基金会的开源操作系统 Linux 所使用的内核。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连接到基于 Web 的管理界面并请求 URLs 从而检索敏感信息，提升权限，导致拒绝服务等。

CNVD 收录的相关漏洞包括：Linux kernel 竞争条件漏洞（CNVD-2022-74084）、Linux kernel 拒绝服务漏洞（CNVD-2022-74086、CNVD-2022-74090）、Linux kernel 访问控制错误漏洞（CNVD-2022-74085）、Linux Kernel 竞争条件问题漏洞（CNVD-2022-74088、CNVD-2022-74091）、Linux kernel 资源管理错误漏洞（CNVD-2022-74087、CNVD-2022-74092）。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-2022-74084

https://www.cnvd.org.cn/flaw/show/CNVD-2022-74086

https://www.cnvd.org.cn/flaw/show/CNVD-2022-74085

https://www.cnvd.org.cn/flaw/show/CNVD-2022-74088

https://www.cnvd.org.cn/flaw/show/CNVD-2022-74087

https://www.cnvd.org.cn/flaw/show/CNVD-2022-74090

https://www.cnvd.org.cn/flaw/show/CNVD-2022-74092

https://www.cnvd.org.cn/flaw/show/CNVD-2022-74091

2、Apache 产品安全漏洞

Apache Commons Text 是美国阿帕奇（Apache）基金会的一个专注于字符串算法的库。Apache Commons JXPath 是一种 XPath1.0 的基于 Java 的实现。Apache Kafka 是一

套开源的分布式流媒体平台。该平台能够获取实时数据，用于构建对数据流的变化进行实时反应的应用程序。Apache XML Graphics Batik 是一套基于 Java 的主要用于处理 SVG 格式图像的应用程序。Apache SOAP 是用作客户端库来调用其他地方可用的 SOAP 服务，也可以用作服务器端工具来实现 SOAP 可访问服务。Apache Airflow 是一套用于创建、管理和监控工作流程的开源平台。该平台具有可扩展和动态监控等特点。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞读取任意文件，获取敏感信息，在系统上执行任意代码，造成拒绝服务等。

CNVD 收录的相关漏洞包括：Apache Commons Text 远程代码执行漏洞、Apache Commons JXPath 缓冲区溢出漏洞（CNVD-2022-73687、CNVD-2022-73688、CNVD-2022-73689）、Apache Kafka 拒绝服务漏洞、Apache XML Graphics Batik 服务器端请求伪造漏洞、Apache SOAP XML 外部实体注入漏洞、Apache Airflow 信息泄露漏洞（CNVD-2022-73695）。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-2022-73686
https://www.cnvd.org.cn/flaw/show/CNVD-2022-73687
https://www.cnvd.org.cn/flaw/show/CNVD-2022-73688
https://www.cnvd.org.cn/flaw/show/CNVD-2022-73689
https://www.cnvd.org.cn/flaw/show/CNVD-2022-73691
https://www.cnvd.org.cn/flaw/show/CNVD-2022-73692
https://www.cnvd.org.cn/flaw/show/CNVD-2022-73694
https://www.cnvd.org.cn/flaw/show/CNVD-2022-73695

3、 Microsoft 产品安全漏洞

Microsoft Windows 是美国微软（Microsoft）公司的一种桌面操作系统。本周，上述产品被披露存在远程代码执行漏洞，攻击者可利用漏洞在目标主机上执行代码。

CNVD 收录的相关漏洞包括：Microsoft Windows LDAP 远程代码执行漏洞（CNVD-2022-72854、CNVD-2022-72860、CNVD-2022-72853、CNVD-2022-72857、CNVD-2022-72856、CNVD-2022-72855、CNVD-2022-72859、CNVD-2022-72858）。其中，“Microsoft Windows LDAP 远程代码执行漏洞（CNVD-2022-72857、CNVD-2022-72856、CNVD-2022-72855、CNVD-2022-72859）”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-2022-72854
https://www.cnvd.org.cn/flaw/show/CNVD-2022-72853
https://www.cnvd.org.cn/flaw/show/CNVD-2022-72857
https://www.cnvd.org.cn/flaw/show/CNVD-2022-72856

https://www.cnvd.org.cn/flaw/show/CNVD-2022-72855

https://www.cnvd.org.cn/flaw/show/CNVD-2022-72860

https://www.cnvd.org.cn/flaw/show/CNVD-2022-72859

https://www.cnvd.org.cn/flaw/show/CNVD-2022-72858

4、F5 产品安全漏洞

F5 BIG-IP 是 F5 公司的一款集成了网络流量编排、负载均衡、智能 DNS，远程接入策略管理等功能的应用交付平台。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞在当前登录用户的上下文中运行 JavaScript，导致拒绝服务。

CNVD 收录的相关漏洞包括：F5 BIG-IP 输入验证错误漏洞（CNVD-2022-72753）、F5 BIG-IP 代码问题漏洞（CNVD-2022-72752、CNVD-2022-72755、CNVD-2022-72756、CNVD-2022-72256）、F5 BIG-IP 跨站脚本漏洞（CNVD-2022-72758）、F5 BIG-IP 资源管理错误漏洞（CNVD-2022-72757、CNVD-2022-72759）。其中，除“F5 BIG-IP 跨站脚本漏洞（CNVD-2022-72758）”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-2022-72256

https://www.cnvd.org.cn/flaw/show/CNVD-2022-72753

https://www.cnvd.org.cn/flaw/show/CNVD-2022-72752

https://www.cnvd.org.cn/flaw/show/CNVD-2022-72755

https://www.cnvd.org.cn/flaw/show/CNVD-2022-72758

https://www.cnvd.org.cn/flaw/show/CNVD-2022-72757

https://www.cnvd.org.cn/flaw/show/CNVD-2022-72756

https://www.cnvd.org.cn/flaw/show/CNVD-2022-72759

5、Omron CX-Position 越界写入漏洞

Omron CX-Position 是日本 Omron 公司的一个位置控制软件。简化了位置控制的各个方面，从创建/编辑位置控制单元（NC 单元）中使用的数据到在线通信和监控操作。本周，Omron CX-Position 被披露存在越界写入漏洞。攻击者可利用该漏洞导致越界写入并执行任意代码。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-2022-73188

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.htm

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-2022	WordPress 插件 flo-launch 访	高	厂商已发布了漏洞修复程序，请及

-72703	问控制错误漏洞		时关注更新：https://wpscan.com/vulnerability/822cac2c-decd-4aa4-9e8e-1ba2d0c080ce
CNVD-2022-73123	Apache HTTP Server 数据伪造问题漏洞（CNVD-2022-73123）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://httpd.apache.org/security/vulnerabilities_24.html
CNVD-2022-73348	OpenSSL 远程代码执行漏洞（CNVD-2022-73348）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.openssl.org/source/mirror.html
CNVD-2022-73495	Quicklert for Digium SQL 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://quicklert.com
CNVD-2022-73696	Huawei 多款产品命令注入漏洞	高	目前厂商已发布升级补丁以修复漏洞，详情请关注厂商主页：https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200902-01-command-en
CNVD-2022-74074	Online Diagnostic Lab Management System SQL 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.sourcecodester.com/php/15129/online-diagnostic-lab-management-system-php-free-source-code.html
CNVD-2022-74080	easyii CMS 跨站请求伪造漏洞（CNVD-2022-74080）	高	目前厂商已提供补丁或者升级程序，建议使用此软件的用户随时关注厂商的主页以获取最新版本：https://github.com/noumo/easyii/issues/222
CNVD-2022-74078	Apple tvOS 资源管理错误漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://support.apple.com/zh-cn/HT213487
CNVD-2022-74094	Hospital Management System SQL 注入漏洞（CNVD-2022-74094）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/Danie1233/Hospital-Management-System-v1.0-SQLi-3/
CNVD-2022-74093	Hospital Management System SQL 注入漏洞（CNVD-2022-74093）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/Danie1233/Hospital-Management-System-v1.0-SQLi-4/

小结：本周，Linux 产品被披露存在多个漏洞，攻击者可利用漏洞通过连接到基于 Web 的管理界面并请求 URLs 从而检索敏感信息，提升权限，导致拒绝服务等。此外，Apache、Microsoft、F5 等多款产品被披露存在多个漏洞，攻击者可利用漏洞读取任意文件，获取敏感信息，在目标主机上执行代码，导致拒绝服务等。另外，Omron CX-Position 被披露存在越界写入漏洞。攻击者可利用漏洞导致越界写入并执行任意代码。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、Online Project Time Management System SQL 注入漏洞

验证描述

Online Project Time Management System 是一个基于网络的在线项目时间管理系统，它为某个公司的员工提供了一个在线平台来报告/记录他们分配的时间或每个项目重新提交的时间。

Online Project Time Management System v1.0 版本存在 SQL 注入漏洞，该漏洞源于/ptms/classes/Users.php 中 save_employee 函数中的 id 参数缺少对外部输入 SQL 语句的验证，攻击者可利用该漏洞执行非法 SQL 命令窃取数据库敏感数据。

验证信息

POC 链接：https://www.exploit-db.com/exploits/50682

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2022-73496

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. OpenSSL 3 漏洞补丁释出，漏洞等级略降

备受瞩目的 OpenSSL 3 漏洞补丁释出，漏洞等级从之前被认为与 Heartbleed 漏洞相当的“高危”降为“高”。

参考链接：https://www.solidot.org/story?sid=73236

2. Checkmk IT 基础设施监控软件中报告了多个漏洞

Checkmk IT Infrastructure 监控软件中披露了多个漏洞，这些漏洞可以被未经身份验证的远程攻击者链接在一起，以在运行 Checkmk 2.1.0p10 及更低版本的服务器上执

行代码。

参考链接：https://thehackernews.com/2022/11/multiple-vulnerabilities-reported-in.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