国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2022 年 08 月 01 日-2022 年 08 月 07 日 **2022 年第 31 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 550 个，其中高危漏洞 202 个、中危漏洞 292 个、低危漏洞 56 个。漏洞平均分值为 6.11。本周收录的漏洞中，涉及 0day 漏洞 312 个（占 57%），其中互联网上出现“Nsasoft US LLC SpotAuditor 拒绝服务漏洞、Totolink A3600R 缓冲区溢出漏洞”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 6731 个，与上周（7660 个）环比减少 12%。

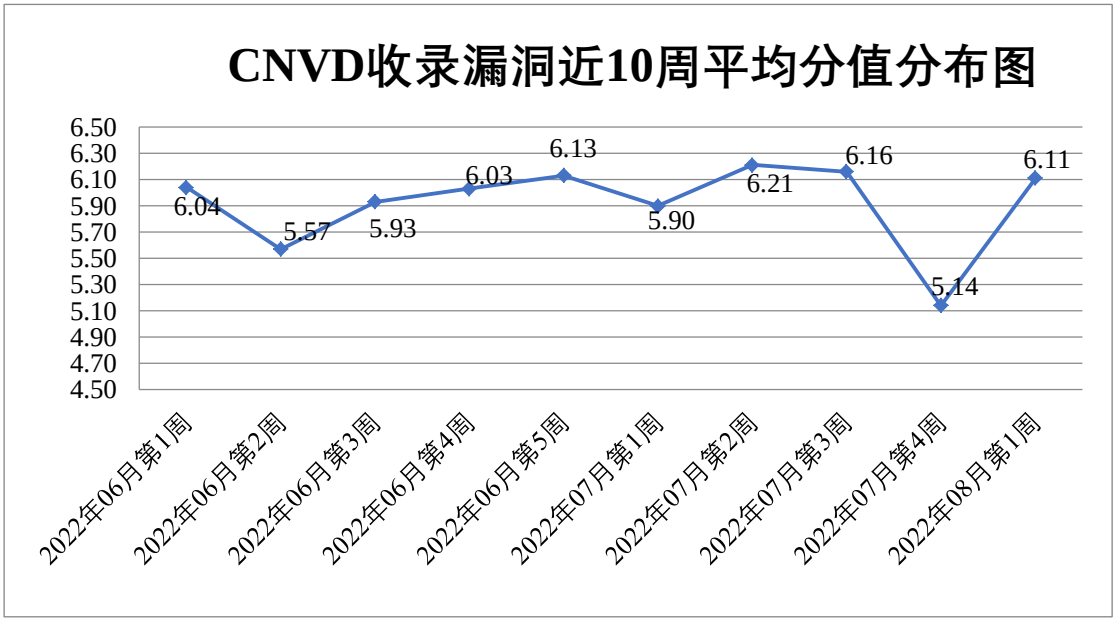

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 24 起，向基础电信企业通报漏洞事件 9 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 285 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 42 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 53 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：

郑州维维信息技术有限公司、浙江大华技术股份有限公司、长沙友点软件科技有限公司、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、新天科技股份有限公司、夏普商贸（中国）有限公司、西安大西信息科技有限公司、微软（中国）有限公司、网神信息技术(北京)股份有限公司、同方计算机（苏州）有限公司、腾讯安全应急响应中心、索尼（中国）有限公司、松下电器(中国)有限公司、四平市九州易通科技有限公司、四川万博教育软件股份有限公司、深圳市优威视讯科技股份有限公司、深圳市万网博通科技有限公司、深圳市绿联科技股份有限公司、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、上海穆云智能科技有限公司、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、山石网科通信技术股份有限公司、锐捷网络股份有限公司、麒麟软件有限公司、奇安信科技集团股份有限公司、迈普通信技术股份有限公司、敬业钢铁有限公司、金山软件股份有限公司、吉翁电子（深圳）有限公司、恒锋信息科技股份有限公司、杭州叙简科技股份有限公司、杭州新中大科技股份有限公司、杭州海康威视数字技术股份有限公司、海南赞赞网络科技有限公司、广州图创计算机软件开发有限公司、广州三晶电气股份有限公司、广州酷狗计算机科技有限公司、佛山市慧动科技有限公司、东莞市通天星软件科技有限公司、鼎捷软件股份有限公司、大唐电信科技股份有限公司、成都云祺科技有限公司、畅捷通信息技术股份有限公司、北京智慧远景科技产业有限公司、北京致远互联软件股份有限公司、北京星网锐捷网络技术有限公司、北京网御星云信息技术有限公司、北京万户软件技术有限公司、北京通达信科科技有限公司、北京拓尔思信息技术股份有限公司、北京明朝万达科技股份有限公司、北京久其云福科技有限公司、北京国炬信息技术有限公司、北京富邦融信国际贸易有限公司、北京传奇华育教育科技股份有限公司、北京百卓网络技术有限公司、北京百度网讯科技有限公司、北京安博通科技股份有限公司、百纳互动网络（福建）有限公司、安徽皖通邮电股份有限公司、信呼、The Apache Software Foundation、Python Software Foundation、book-manager、Apereo 和 ANGLIA DESIGN LIMITED。

本周，CNVD 发布了《F5 公司发布 2022 年 8 月安全更新》。详情参见 CNVD 网站公告内容。

https://www.cnvd.org.cn/webinfo/show/7961

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、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、杭州安恒信息技术股份有限公司、恒安嘉新（北京）科技股份公司等单位报送公开收集的漏洞数量较多。北京华顺信安科技有限公司、河南信安世纪科技有限公司、山石网科通信技术股份有限公司、河南东方云盾信息技术有限公司、河南灵创电子科技有限公司、中国银行、苏州棱镜七彩信息科技有限公司、浙江木链物联网科技有限公司、工业和信息化部电子第五研究所、贵州泰若数字科技有限公司、西藏熙安信息技术有限责任公司、重庆都会信息科技有限公司、中国电信股份有限公司上海研究院、上海纽盾科技股份有限公司、平安银河实验室、黑龙江亿林网络股份有限公司、任子行网络技术股份有限公司、江苏国泰新点软件有限公司、内蒙古洞明科技有限公司、南方电网数字电网研究院有限公司、广州易东信息安全技术有限公司、广州安亿信软件科技有限公司、上海端御信息科技有限公司及其他个人白帽子向 CNVD 提交了 6731 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 5185 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）	2502	2502
奇安信网神（补天平台）	1643	1643
三六零数字安全科技集团有限公司	587	587
上海交大	453	453
新华三技术有限公司	269	0
安天科技集团股份有限公司	222	0
北京天融信网络安全技术有限公司	183	2
杭州安恒信息技术股份有限公司	114	49
恒安嘉新（北京）科技股份公司	107	0
北京启明星辰信息安全技术有限公司	61	7
北京知道创宇信息技	18	0

术有限公司		
南京众智维信息科技有限公司	13	13
内蒙古奥创科技有限公司	4	4
北京智游网安科技有限公司	4	4
北京神州绿盟科技有限公司	2	2
北京华顺信安科技有限公司	701	5
河南信安世纪科技有限公司	399	399
山石网科通信技术股份有限公司	29	29
河南东方云盾信息技术有限公司	28	28
F5	21	0
杭州迪普科技股份有限公司	14	0
河南灵创电子科技有限公司	10	10
中国银行	4	4
苏州棱镜七彩信息科技有限公司	4	4
浙江木链物联网科技有限公司	3	3
工业和信息化部电子第五研究所	3	3
贵州泰若数字科技有限公司	3	3
西藏熙安信息技术有限责任公司	2	2
重庆都会信息科技有限公司	2	2

中国电信股份有限公司上海研究院	2	2
上海纽盾科技股份有限公司	2	2
平安银河实验室	2	2
黑龙江亿林网络股份有限公司	2	2
任子行网络技术股份有限公司	1	1
江苏国泰新点软件有限公司	1	1
内蒙古洞明科技有限公司	1	1
南方电网数字电网研究院有限公司	1	1
广州易东信息安全技术有限公司	1	1
广州安亿信软件科技有限公司	1	1
上海端御信息科技有限公司	1	1
CNCERT 四川分中心	6	6
CNCERT 内蒙古分中心	1	1
个人	951	951
报送总计	8378	6731

本周漏洞按类型和厂商统计

本周，CNVD 收录了 550 个漏洞。WEB 应用 203 个，应用程序 195 个，网络设备（交换机、路由器等网络端设备）103 个，操作系统 30 个，智能设备（物联网终端设备）11 个，数据库 5 个，安全产品 3 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	203

应用程序	195
网络设备（交换机、路由器等网络端设备）	103
操作系统	30
智能设备（物联网终端设备）	11
数据库	5
安全产品	3

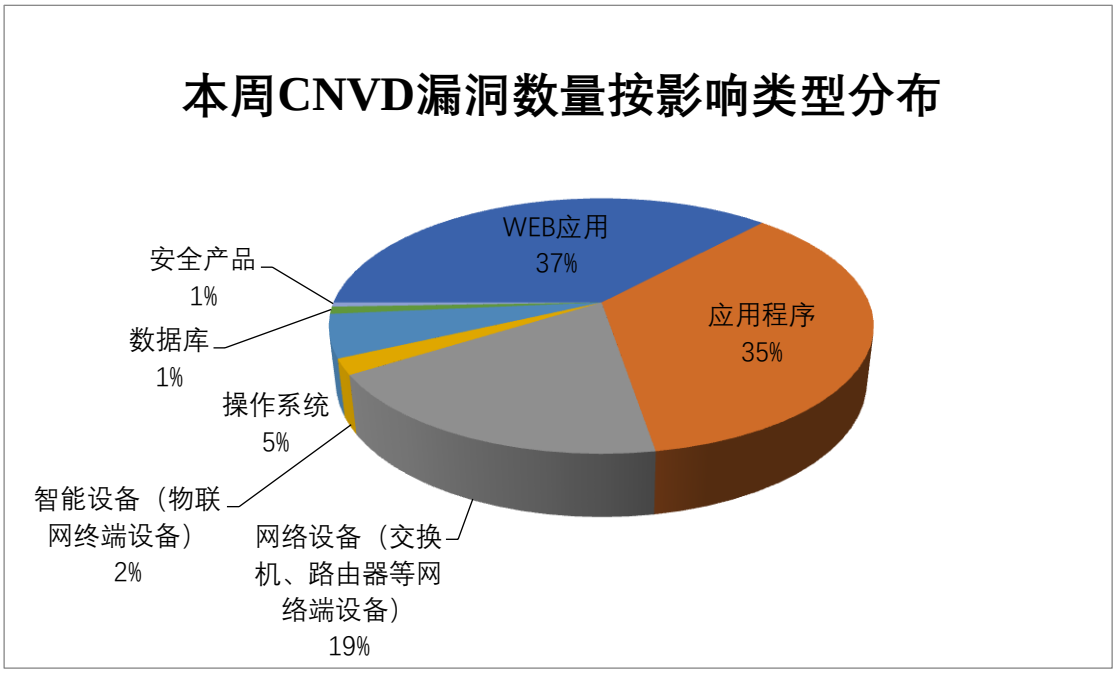

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Jenkins、IBM、Tenda 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	Jenkins	33	6%
2	IBM	26	5%
3	Tenda	20	4%
4	F5	19	4%
5	Cisco	17	3%
6	Pexip	17	3%
7	友讯电子设备（上海）有限公司	16	3%
8	TOTOLINK	13	2%
9	WordPress	13	2%
10	其他	376	68%

本周行业漏洞收录情况

本周，CNVD 收录了 82 个电信行业漏洞，30 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，“Cisco Small Business 缓冲区溢出漏洞（CNVD-2022-54905）、MongoDB 缓冲区溢出漏洞”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/

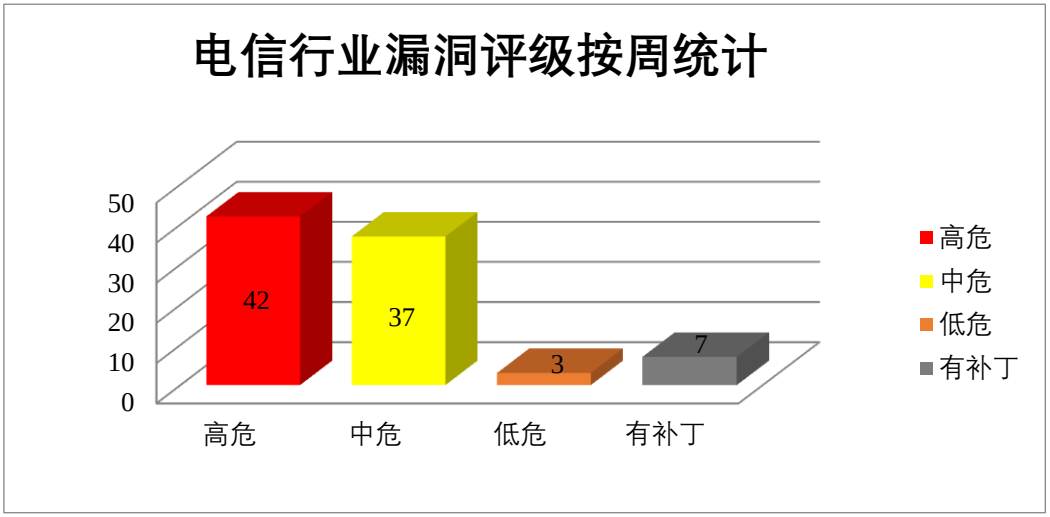

图 3 电信行业漏洞统计

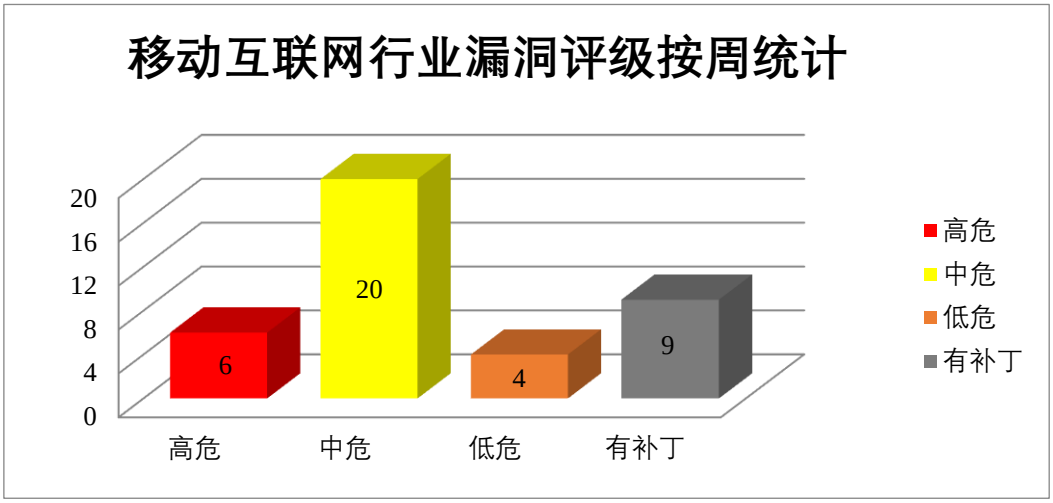

图 4 移动互联网行业漏洞统计

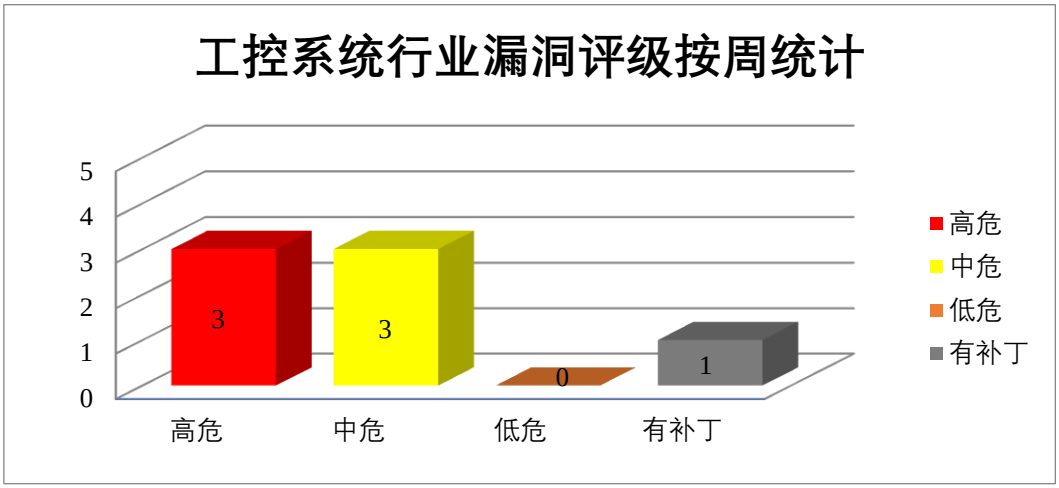

图 5 工控系统行业漏洞统计

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、 Cisco 产品安全漏洞

Cisco Nexus Dashboard 是美国思科（Cisco）公司的一个单一控制台。能够简化数据中心网络的运营和管理。Cisco IOS XE 是一套为其网络设备开发的操作系统。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拒绝服务，权限提升等。

CNVD 收录的相关漏洞包括：Cisco Nexus Dashboard 访问控制错误漏洞、Cisco Nexus Dashboard 权限提升漏洞（CNVD-2022-54958、CNVD-2022-54959）、Cisco Nexus Dashboard 操作系统命令注入漏洞、Cisco IOS XE AVC-FNF 拒绝服务漏洞、Cisco IOS XE Wireless Controller software 拒绝服务漏洞、Cisco IOS XE 权限提升漏洞（CNVD-2022-55150）、Cisco IOS XE AppNav-XE 拒绝服务漏洞。其中，除“Cisco Nexus Dashboard 权限提升漏洞（CNVD-2022-54958、CNVD-2022-54959）”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-2022-54909

https://www.cnvd.org.cn/flaw/show/CNVD-2022-54959

https://www.cnvd.org.cn/flaw/show/CNVD-2022-54958

https://www.cnvd.org.cn/flaw/show/CNVD-2022-54960

https://www.cnvd.org.cn/flaw/show/CNVD-2022-55147

https://www.cnvd.org.cn/flaw/show/CNVD-2022-55145

https://www.cnvd.org.cn/flaw/show/CNVD-2022-55150

https://www.cnvd.org.cn/flaw/show/CNVD-2022-55148

2、 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。F5 BIG-IP APM Edge Client for Windows 是一款客户端访问控制认证接入客户端应用程序。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拒绝服务。

CNVD 收录的相关漏洞包括：F5 BIG-IP APM 和 F5 SSL Orchestrator 拒绝服务漏洞、F5 BIG-IP HTTP MRF 拒绝服务漏洞、F5 BIG-IP APM 空指针指针解引用漏洞、F5 BIG-IP 消息路由 MQTT 拒绝服务漏洞、F5 BIG-IP HTTP2 配置文件拒绝服务漏洞、F5 BIG-IP TLS 1.3 iRule 空指针解引用漏洞、F5 BIG-IP TMM ClientSSL 配置文件拒绝服务漏洞、F5 BIG-IP TMM iRule 拒绝服务漏洞。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-2022-55179
https://www.cnvd.org.cn/flaw/show/CNVD-2022-55178
https://www.cnvd.org.cn/flaw/show/CNVD-2022-55185
https://www.cnvd.org.cn/flaw/show/CNVD-2022-55184
https://www.cnvd.org.cn/flaw/show/CNVD-2022-55183
https://www.cnvd.org.cn/flaw/show/CNVD-2022-55182
https://www.cnvd.org.cn/flaw/show/CNVD-2022-55181
https://www.cnvd.org.cn/flaw/show/CNVD-2022-55186

3、IBM 产品安全漏洞

IBM CICS TX Standard and Advanced 是美国 IBM 公司的综合的、单一的事务运行时包。可以为独立应用程序提供云原生部署模型。IBM Cognos Analytics 是一套商业智能软件。该软件包括报表、仪表板和记分卡等，并可通过分析关键因素与关键人等内容，协助企业调整决策。IBM Financial Transaction Manager for Digital Payments 是一款金融事务管理器。该产品主要用于监控、跟踪和报告金融支付和交易。IBM Curam Social Program Management 是一种业务和技术解决方案，可在动态可配置架构之上提供预构建的健康和社交计划组件、业务流程、工具集和界面。IBM Security Verify Information Queue（使用首字母缩写词“ISIQ”）是一个跨产品集成商，利用 Kafka 技术和发布/订阅模型在 IBM Security 产品之间集成数据。IBM WebSphere Application Server（WAS）是一款应用服务器产品。该产品是 JavaEE 和 Web 服务应用程序的平台，也是 IBM WebSphere 软件平台的基础。IBM InfoSphere InformationServer 是一种数据集成软件平台，可以帮助企业从分散在系统中的复杂的异类信息中获得更多价值。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敏感信息，上传任意文件，导致任意命令执行等。

CNVD 收录的相关漏洞包括：IBM CICS TX Standard and Advanced 操作系统命

令注入漏洞、IBM Cognos Analytics 文件上传漏洞、IBM Financial Transaction Manager for Digital Payments SQL 注入漏洞、IBM Curam Social Program Management 代码问题漏洞（CNVD-2022-54649）、IBM Security Verify Information Queue 信息泄露漏洞（CNVD-2022-54888）、IBM WebSphere Application Server 信息泄露漏洞（CNVD-2022-54962）、IBM InfoSphere Information Server SQL 注入漏洞（CNVD-2022-54979）、IBM WebSphere Application Server 跨站脚本漏洞。其中，除“IBM WebSphere Application Server 信息泄露漏洞（CNVD-2022-54962）、IBM WebSphere Application Server 跨站脚本漏洞”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-2022-54640

https://www.cnvd.org.cn/flaw/show/CNVD-2022-54642

https://www.cnvd.org.cn/flaw/show/CNVD-2022-54646

https://www.cnvd.org.cn/flaw/show/CNVD-2022-54649

https://www.cnvd.org.cn/flaw/show/CNVD-2022-54888

https://www.cnvd.org.cn/flaw/show/CNVD-2022-54962

https://www.cnvd.org.cn/flaw/show/CNVD-2022-54979

https://www.cnvd.org.cn/flaw/show/CNVD-2022-55504

4、 Oracle 产品安全漏洞

Oracle Solaris 是美国甲骨文（Oracle）公司的一套 UNIX 操作系统。Oracle ZFS Storage Appliance 是一个支持闪存、PB 级文件存储并内置 Oracle 数据库的存储设备。Oracle Enterprise Manager Base Platform 是一套本地管理平台。该平台主要用于管理 Oracle 产品部署。Oracle Financial Services Applications 是一套金融服务软件。该产品包括核心银行、网上银行和财产管理等。FLEXCUBE Universal Banking 是其中的一个互联网和移动银行业务解决方案组件。Oracle WebLogic Server 是一款适用于云环境和传统环境的应用服务中间件，它提供了一个现代轻型开发平台，支持应用从开发到生产的整个生命周期管理，并简化了应用的部署和管理。Oracle Essbase 是一个应用软件。使组织能够使用假设分析和数据可视化工具从多维数据集中快速生成洞察力。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对 Enterprise Manager Base Platform 可访问数据的更新、插入或删除，Oracle Solaris 挂起或频繁重复崩溃等。

CNVD 收录的相关漏洞包括：Oracle Solaris 拒绝服务漏洞（CNVD-2022-54629）、Oracle ZFS Storage Appliance 输入验证错误漏洞、Oracle Solaris 输入验证错误漏洞（CNVD-2022-54631）、Oracle Solaris 拒绝服务漏洞（CNVD-2022-54630）、Oracle Enterprise Manager Base Platform 输入验证错误漏洞、Oracle Financial Services Applications 输入验证错误漏洞、Oracle WebLogic Server Core 组件输入验证错误漏洞、Oracle Essbase 信息泄露漏洞。其中，“Oracle Solaris 拒绝服务漏洞（CNVD-2022-54629）、Or

acle Solaris 输入验证错误漏洞（CNVD-2022-54631）、Oracle Enterprise Manager Base Platform 输入验证错误漏洞”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-2022-54629

https://www.cnvd.org.cn/flaw/show/CNVD-2022-54632

https://www.cnvd.org.cn/flaw/show/CNVD-2022-54631

https://www.cnvd.org.cn/flaw/show/CNVD-2022-54630

https://www.cnvd.org.cn/flaw/show/CNVD-2022-54637

https://www.cnvd.org.cn/flaw/show/CNVD-2022-54635

https://www.cnvd.org.cn/flaw/show/CNVD-2022-54634

https://www.cnvd.org.cn/flaw/show/CNVD-2022-54633

5、Google Android 安全绕过漏洞（CNVD-2022-54478）

Google Android 是美国谷歌（Google）公司的一套以 Linux 为基础的开源操作系统。本周，Google Android 被披露存在安全绕过漏洞。攻击者可利用该漏洞绕过身份验证并获得访问权限。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-2022-54478

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-2022-54652	TotoLink A3100R 命令注入漏洞（CNVD-2022-54652）	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/170/ids/36.html
CNVD-2022-54889	Adobe Acrobat Reader 缓冲区溢出漏洞（CNVD-2022-54889）	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/acrobat/apsb22-16.html
CNVD-2022-54895	Adobe InDesign 缓冲区溢出漏洞（CNVD-2022-54895）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://helpx.adobe.com/security/products/indesign/apsb22-30.html
CNVD-2022-54899	Vim 缓冲区溢出漏洞（CNVD-2022-54899）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/vim/vim/commit/5fa9f23a63651a8abdb074b4fc2ec9b1a

			dc6b089
CNVD-2022-54903	OpenEMR 访问控制错误漏洞（CNVD-2022-54903）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/openemr/openemr/commit/871ae5198d8ca18fd17257ae7c5c906a52dca908
CNVD-2022-54911	Moodle 输入验证错误漏洞（CNVD-2022-54911）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://moodle.org/mod/forum/discuss.php?d=436456
CNVD-2022-54910	Apache Xalan 输入验证错误漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://lists.apache.org/thread/12pxy4phsry6c34x2ol4fft6xlho4kyw
CNVD-2022-54912	Adobe Character Animator 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://helpx.adobe.com/security/products/character_animator/apsb22-34.html
CNVD-2022-54915	Moodle 任意文件读取漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://moodle.org/mod/forum/discuss.php?d=436457&parent=1756385
CNVD-2022-55005	Foxit PDF Editor 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：https://www.foxitsoftware.com/support/security-bulletins.php

小结：本周，Cisco 产品被披露存在多个漏洞，攻击者可利用漏洞导致拒绝服务，权限提升等。此外，F5、IBM、Oracle 等多款产品被披露存在多个漏洞，攻击者可利用漏洞获取敏感信息，上传任意文件，导致拒绝服务，任意命令执行等。另外，Google Android 被披露存在安全绕过漏洞。攻击者可利用该漏洞绕过身份验证并获得访问权限。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、Totolink A3600R 缓冲区溢出漏洞

验证描述

TotoLink A3600R 是中国台湾吉翁电子（TotoLink）公司的一款 6 天线 1200M 无线路由器。

Totolink A3600R V4.1.2cu.5182_B20201102 版本存在缓冲区溢出漏洞，该漏洞源于

在 infostat.cgi 的 fread 函数中包含堆栈器溢出，攻击者可利用该漏洞通过参数 CONTENT_LENGTH 导致拒绝服务 (DoS)。

验证信息

POC 链接：https://github.com/molezsbd/iot-cve/tree/master/totolink/a3600r

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2022-54650

信息提供者

京东科技信息技术有限公司

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. DrayTek 爆出 RCE 漏洞，影响旗下 29 个型号的路由器

研究人员发现一个远程代码执行 (RCE) 漏洞，该漏洞会对 29 种型号的 DrayTek Vigor 商业路由器产生严重影响。

参考链接：https://www.freebuf.com/news/341124.html

2. VMware 敦促管理员修补身份验证绕过漏洞

VMware 今天警告管理员修补一个身份验证绕过安全漏洞，该漏洞会影响多个产品中的本地域用户，并使未经身份验证的攻击者能够获得管理员权限。

参考链接：https://www.bleepingcomputer.com/news/security/vmware-urges-admins-to-patch-critical-auth-bypass-bug-immediately/

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