国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2022 年 03 月 07 日-2022 年 03 月 13 日 **2022 年第 10 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 578 个，其中高危漏洞 199 个、中危漏洞 333 个、低危漏洞 46 个。漏洞平均分值为 5.99。本周收录的漏洞中，涉及 0day 漏洞 303 个（占 52%），其中互联网上出现“TOTOLink A830R 命令注入漏洞、Home Owners Collection 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 4325 个，与上周（4175 个）环比增加 4%。

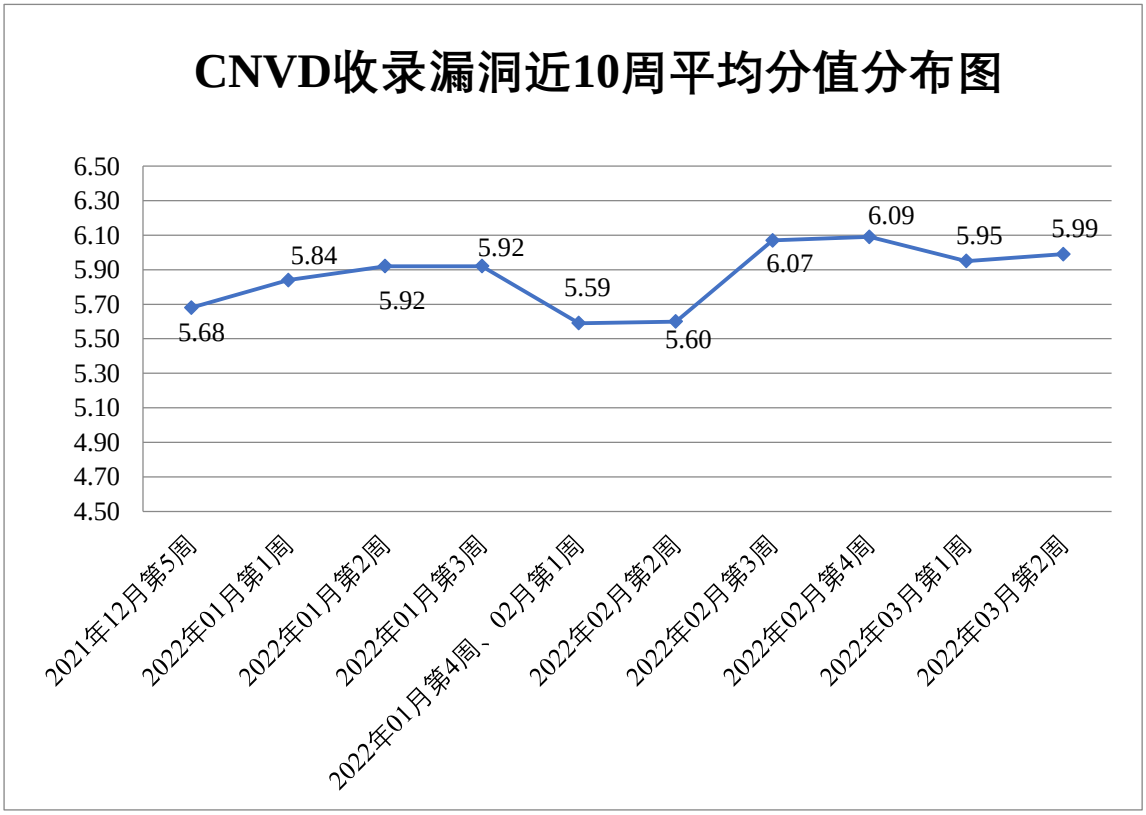

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 21 起，向基础电信企业通报漏洞事件 26 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 809 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 75 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 87 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：

遵义欣腾达信息技术有限公司、紫光软件系统有限公司、淄博闪灵网络科技有限公司、珠海新华通软件股份有限公司、珠海金山办公软件有限公司、长沙德尚网络科技有限公司、友讯电子设备（上海）有限公司、艺库网络科技有限公司、兄弟（中国）商业有限公司、新天科技股份有限公司、暇光软件科技（上海）有限公司、西安紫云羚网络科技有限责任公司、西安启莱软件科技有限公司、武汉达梦数据库股份有限公司、温州互引信息技术有限公司、维沃移动通信有限公司、微软（中国）有限公司、统信软件技术有限公司、天津神舟通用数据技术有限公司、天津奥兴同创广告传媒有限公司、台达电子企业管理(上海)有限公司、四创科技有限公司、深圳雅科网络科技有限公司、深圳市英威腾电气股份有限公司、深圳市迅雷网络技术有限公司、深圳市吉祥腾达科技有限公司、深圳市博思协创网络科技有限公司、上海居亦科技发展有限公司、上海金慧软件有限公司、上海汉得信息技术股份有限公司、上海海典软件股份有限公司、上海孚盟软件有限公司、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、上海贝锐信息科技股份有限公司、上海艾泰科技有限公司、熵基科技股份有限公司、陕西亚创科技有限公司、山脉科技股份有限公司、厦门四信通信科技有限公司、青岛中翔汇智网络科技有限公司、青岛商至信网络科技有限公司、普元信息技术股份有限公司、普联技术有限公司、宁波中茂网络科技有限公司、蓝网科技股份有限公司、江西铭软科技有限公司、吉翁电子（深圳）有限公司、惠普贸易（上海）有限公司、杭州伊柯夫科技有限公司、杭州灵伴科技有限公司、杭州可道云网络有限公司、广州市保伦电子有限公司、广州巨杉软件开发有限公司、广东省深圳国泰安教育技术有限公司、高德软件有限公司、东芝（中国）有限公司、成都泰盟软件有限公司、畅捷通信息技术股份有限公司、北京星网锐捷网络技术有限公司、北京五指互联科技有限公司、北京通达信科科技有限公司、北京赛普智成科技有限公司、北京人大金仓信息技术股份有限公司、北京卡巴斯基网络安全技术有限公司、北京九思协同软件有限公司、北京建设数字科技股份有限公司、北京集慧智佳知识产权管理咨询股份有限公司、北京国栋科技有限公司、北京东方通科技股份有限公司、北京奥特美克科技股份有限公司、北大医疗信息技术有限公司、安徽阳光心健科技发展有限公司、安徽容知日新科技股份有限公司、安徽交欣科技股份有限公

司、腾讯安全应急响应中心、码坤科技、桂林市七星区码坤网络科技工作室、zzzcms、The Apache Software Foundation、Skylink、SemCms、Prolink、phpems、PhpaaCMS、nginxWebUI、Kong Inc.、emlog、DataGear、Arista Networks、Alpha Technologies 和 Adobe。

本周，CNVD 发布了《Microsoft 发布 2022 年 3 月安全更新》。详情参见 CNVD 网站公告内容。

https://www.cnvd.org.cn/webinfo/show/7481

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、厦门服云信息科技有限公司、恒安嘉新（北京）科技股份公司、北京神州绿盟科技有限公司等单位报送公开收集的漏洞数量较多。天津偕行科技有限公司、杭州默安科技有限公司、北京山石网科信息技术有限公司、上海纽盾科技股份有限公司、广州百蕴启辰科技有限公司、贵州多彩宝互联网服务有限公司、华鲁数智信息技术（北京）有限公司、重庆都会信息科技、内蒙古洞明科技有限公司、江苏保旺达软件技术有限公司、南京树安信息技术有限公司、开元华创科技集团、山东云天安全技术有限公司、贵州泰若数字科技有限公司、浙江大学控制科学与工程学院、深圳市魔方安全科技有限公司、北京机沃科技有限公司、贵州亨达集团信息安全技术有限公司、河南灵创电子科技有限公司、星云博创科技有限公司、快页信息技术有限公司、长春嘉诚信息技术股份有限公司、杭州海康威视数字技术股份有限公司、广西等保安全测评有限公司、河南信安世纪科技有限公司、浙江御安信息技术有限公司、山东新潮信息技术有限公司、北京威努特技术有限公司、博智安全科技股份有限公司、上海上讯信息技术股份有限公司、内蒙古迅如信息安全科技有限公司、交通运输信息安全中心有限公司、思而听网络科技有限公司、海南神州希望网路有限公司、陕西青山四纪信息技术有限公司、深圳开源互联网安全技术有限公司、武汉安域信息安全技术有限公司、北京远禾科技有限公司及其他个人白帽子向 CNVD 提交了 4325 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）、上海交大和奇安信网神（补天平台）向 CNVD 共享的白帽子报送的 2439 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）	1338	1338
上海交大	642	642
奇安信网神（补天平台）	459	459
新华三技术有限公司	306	0

安天科技集团股份有限公司	193	0
厦门服云信息科技有限公司	176	0
恒安嘉新（北京）科技股份公司	126	0
北京神州绿盟科技有限公司	113	4
北京数字观星科技有限公司	112	0
北京天融信网络安全技术有限公司	111	33
北京华顺信安科技有限公司	109	0
三六零数字安全科技集团有限公司	100	0
西安四叶草信息技术有限公司	84	84
北京启明星辰信息安全技术有限公司	69	10
天津市国瑞数码安全系统股份有限公司	59	0
深信服科技股份有限公司	59	0
杭州安恒信息技术股份有限公司	52	24
中国电信集团系统集成有限责任公司	30	0
远江盛邦（北京）网络安全科技股份有限公司	24	24
南京众智维信息科技有限公司	18	18
北京知道创宇信息技术有限公司	11	0

北京安信天行科技有限公司	10	10
内蒙古云科数据服务股份有限公司	2	2
南京铱迅信息技术股份有限公司	1	1
深圳市腾讯计算机系统有限公司（玄武实验室）	1	1
亚信科技（成都）有限公司	73	0
天津偕行科技有限公司	56	56
墨菲未来科技(北京)有限公司	48	0
杭州默安科技有限公司	37	37
北京山石网科信息技术有限公司	29	29
上海纽盾科技股份有限公司	29	29
广州百蕴启辰科技有限公司	22	22
贵州多彩宝互联网服务有限公司	21	21
华鲁数智信息技术（北京）有限公司	21	21
西门子（中国）有限公司	20	0
重庆都会信息科技	19	19
内蒙古洞明科技有限公司	18	18
江苏保旺达软件技术有限公司	15	15
南京树安信息技术有	14	14

限公司		
杭州迪普科技股份有限公司	14	0
开元华创科技集团	12	12
山东云天安全技术有限公司	9	9
贵州泰若数字科技有限公司	5	5
浙江大学控制科学与工程学院	4	4
深圳市魔方安全科技有限公司	4	4
北京机沃科技有限公司	3	3
贵州亨达集团信息安全技术有限公司	3	3
河南灵创电子科技有限公司	3	3
星云博创科技有限公司	3	3
快页信息技术有限公司	3	3
长春嘉诚信息技术股份有限公司	3	3
杭州海康威视数字技术股份有限公司	2	2
广西等保安全测评有限公司	2	2
河南信安世纪科技有限公司	2	2
浙江御安信息技术有限公司	1	1
山东新潮信息技术有限公司	1	1
北京威努特技术有限	1	1

公司		
博智安全科技股份有限公司	1	1
上海上讯信息技术股份有限公司	1	1
内蒙古迅如信息安全科技有限公司	1	1
交通运输信息安全中心有限公司	1	1
思而听网络科技有限公司	1	1
海南神州希望网路有限公司	1	1
陕西青山四纪信息技术有限公司	1	1
深圳开源互联网安全技术有限公司	1	1
武汉安域信息安全技术有限公司	1	1
北京远禾科技有限公司	1	1
CNCERT 宁夏分中心	16	16
CNCERT 贵州分中心	2	2
CNCERT 四川分中心	1	1
CNCERT 河北分中心	1	1
CNCERT 山东分中心	1	1
个人	1302	1302
报送总计	6035	4325

本周漏洞按类型和厂商统计

本周，CNVD 收录了 578 个漏洞。WEB 应用 189 个，网络设备（交换机、路由器等网络端设备）152 个，应用程序 127 个，操作系统 42 个，数据库 33 个，智能设备（物联网终端设备）28 个，安全产品 7 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	189
网络设备（交换机、路由器等网络端设备）	152
应用程序	127
操作系统	42
数据库	33
智能设备（物联网终端设备）	28
安全产品	7

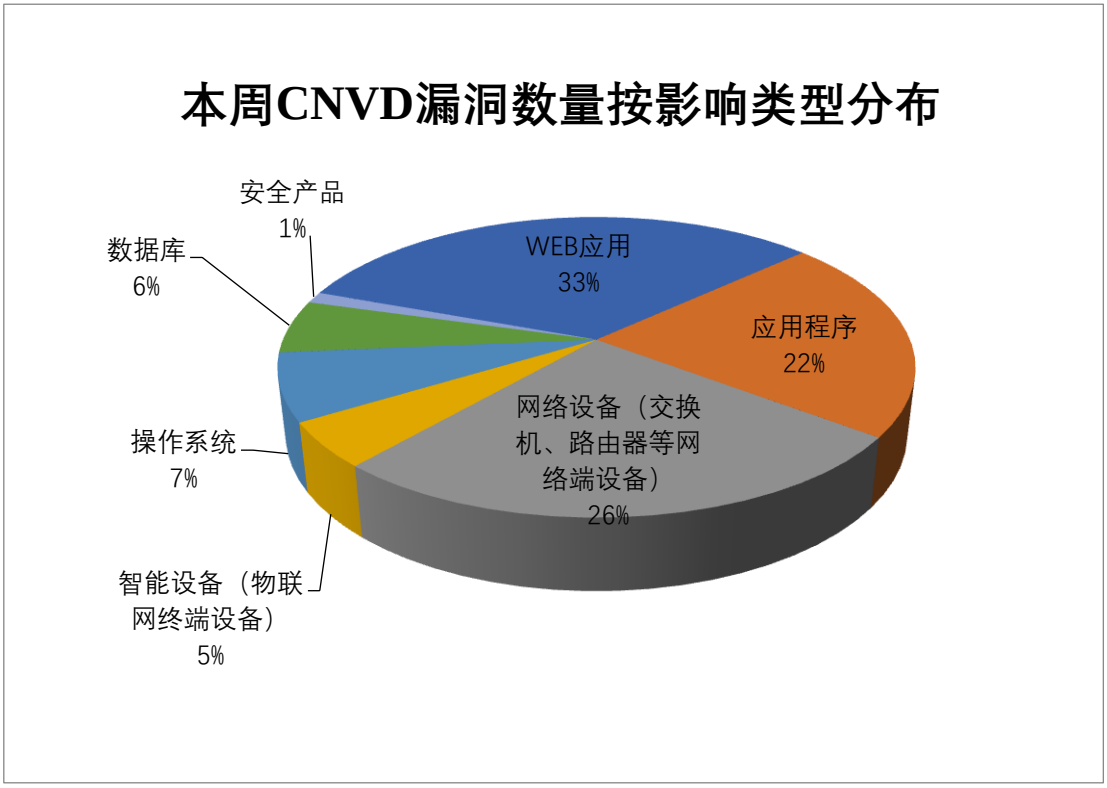

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Oracle、Huawei、TOTOLIN 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	Oracle	44	8%
2	Huawei	31	5%
3	TOTOLINK	26	5%
4	TYPO3	23	4%
5	Siemens	20	3%
6	深圳市吉祥腾达科技有限公司	19	3%
7	Microsoft	15	3%

8	JetBrains	12	2%
9	DELL	11	2%
10	其他	377	65%

本周行业漏洞收录情况

本周，CNVD 收录了 106 个电信行业漏洞，10 个移动互联网行业漏洞，17 个工控行业漏洞（如下图所示）。其中，“Tp-link TL-WA850RE 授权问题漏洞、Tenda Router AX12 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/

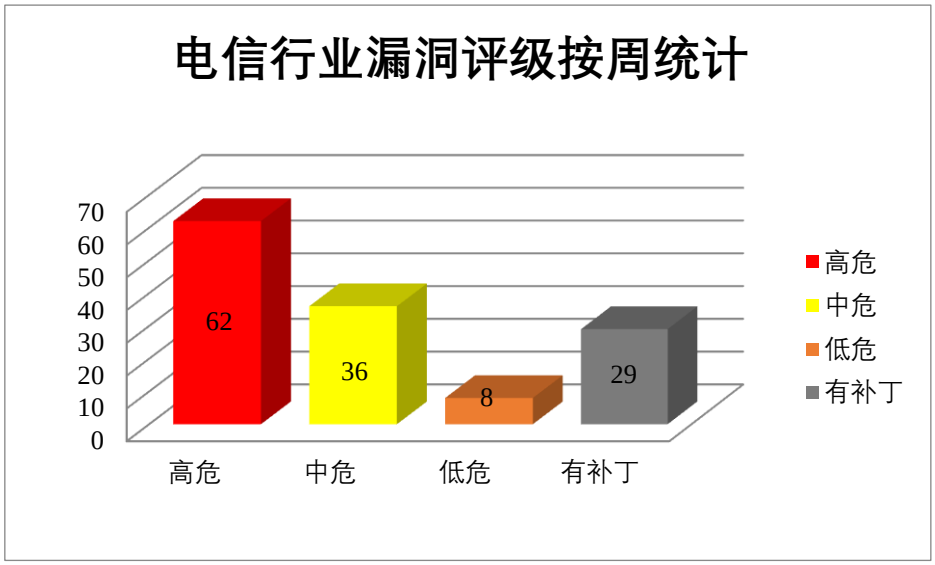

图 3 电信行业漏洞统计

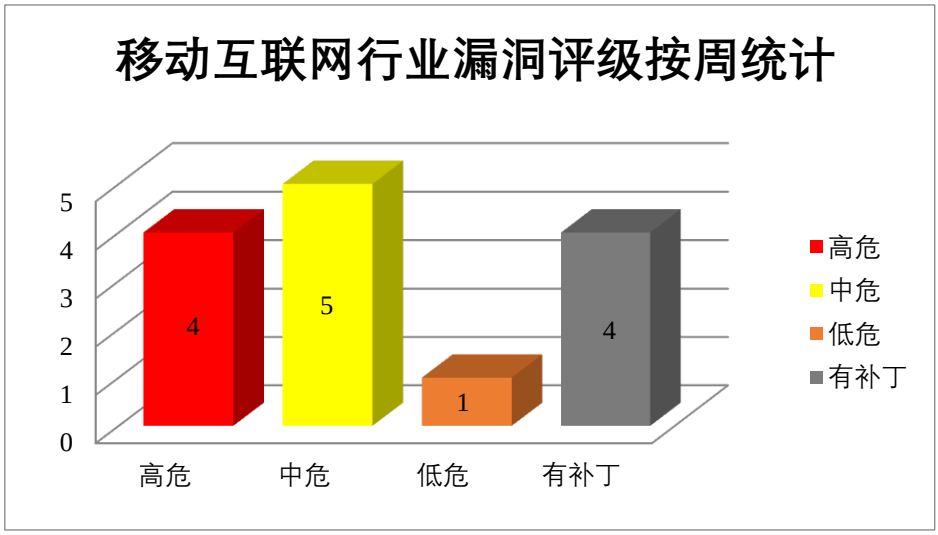

图 4 移动互联网行业漏洞统计

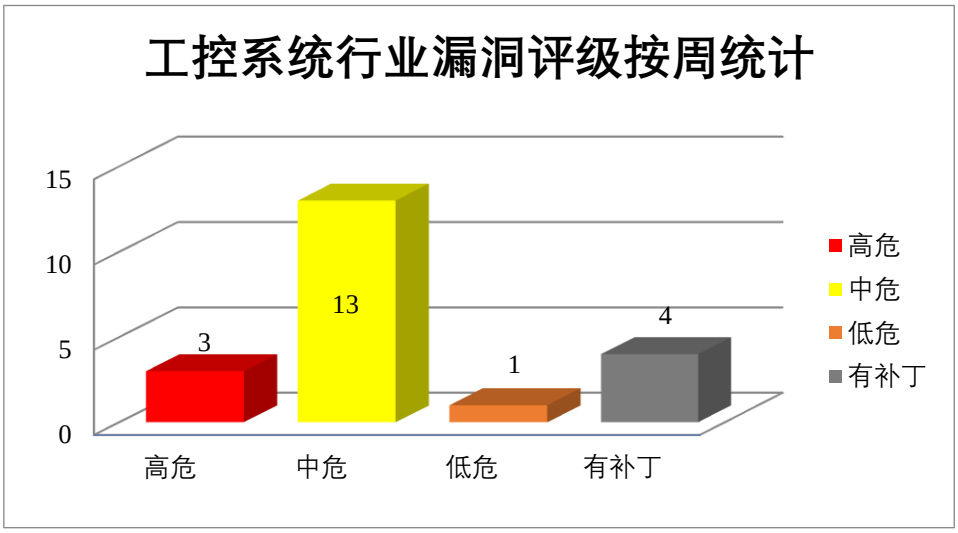

图 5 工控系统行业漏洞统计

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、Huawei 产品安全漏洞

Huawei Emui 是一款基于 Android 开发的移动端操作系统。Magic Ui 是一款基于 Android 开发的移动端操作系统。Huawei AIS-BW80H-00 是中国华为（Huawei）公司的一款智能音箱设备。Huawei HarmonyOS 是中国华为（Huawei）公司的一个操作系统。提供一个基于微内核的全场景分布式操作系统。Huawei PCManager 是中国华为（Huawei）公司的一套电脑管理软件。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随机地址访问，导致内核死机，将特制数据传递给应用程序并在目标系统上执行任意命令等。

CNVD 收录的相关漏洞包括：Huawei Emui 和 Magic UI 整数溢出漏洞、Huawei AIS-BW80H-00 命令注入漏洞、Huawei HarmonyOS 堆溢出漏洞（CNVD-2022-17398）、Huawei HarmonyOS HAL-Ril 数据业务组件越界读取漏洞、Huawei HarmonyOS 数据处理错误型漏洞、Huawei HarmonyOS HwNearbyMain 组件空指针解引用漏洞、Huawei HarmonyOS 空指针解引用漏洞（CNVD-2022-17707）、Huawei PCManager 权限提升题漏洞。其中“Huawei Emui 和 Magic UI 整数溢出漏洞、Huawei HarmonyOS 堆溢出漏洞（CNVD-2022-17398）、Huawei HarmonyOS 空指针解引用漏洞（CNVD-2022-17707）、Huawei PCManager 权限提升题漏洞”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-2022-17394

https://www.cnvd.org.cn/flaw/show/CNVD-2022-17395

https://www.cnvd.org.cn/flaw/show/CNVD-2022-17398

https://www.cnvd.org.cn/flaw/show/CNVD-2022-17403

https://www.cnvd.org.cn/flaw/show/CNVD-2022-17402

https://www.cnvd.org.cn/flaw/show/CNVD-2022-17401

https://www.cnvd.org.cn/flaw/show/CNVD-2022-17707

https://www.cnvd.org.cn/flaw/show/CNVD-2022-17706

2、Oracle 产品安全漏洞

Oracle Enterprise Manager Base Platform 是美国甲骨文（Oracle）公司的一套本地管理平台。该平台主要用于管理 Oracle 产品部署。Oracle Communications 是美国甲骨文（Oracle）公司的一款产品。为服务提供商和企业提供集成通信和云解决方案，以加速他们的数字化转型。Oracle MySQL Server 是美国甲骨文（Oracle）公司的一款关系型数据库。Oracle MySQL Cluster 是美国甲骨文（Oracle）公司开发的一个写可扩展、实时、兼容 ACID 的事务型数据库。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞对关键数据或所有 MySQL Server 可访问数据的未经授权的创建、删除或修改访问，导致 MySQL Server 挂起或频繁重复崩溃等。

CNVD 收录的相关漏洞包括：Oracle Enterprise Session Border Controller 拒绝服务漏洞、Oracle Communications Convergence 授权问题漏洞、Oracle MySQL Server 输入验证错误漏洞（CNVD-2022-17682、CNVD-2022-17681、CNVD-2022-17685、CNVD-2022-17684、CNVD-2022-17683）、Oracle MySQL Cluster 输入验证错误漏洞（CNVD-2022-17688）。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-2022-17339

https://www.cnvd.org.cn/flaw/show/CNVD-2022-17353

https://www.cnvd.org.cn/flaw/show/CNVD-2022-17682

https://www.cnvd.org.cn/flaw/show/CNVD-2022-17681

https://www.cnvd.org.cn/flaw/show/CNVD-2022-17685

https://www.cnvd.org.cn/flaw/show/CNVD-2022-17684

https://www.cnvd.org.cn/flaw/show/CNVD-2022-17683

https://www.cnvd.org.cn/flaw/show/CNVD-2022-17688

3、Siemens 产品安全漏洞

Polarion WebClient for SVN 是一个 SVN 客户端。SINUMERIK MC 是一个用于定制机器解决方案的 CNC 系统。SINUMERIK ONE 是一个数字原生数控系统。Siemens RuggedCom ROS 是德国西门子（Siemens）公司的一套用于 RuggedCom 系列交换机中的操作系统。Siemens SINEC NMS 是德国西门子（Siemens）公司的一个网络管理系统(NMS)，该系统可用于全天候集中监控、管理和配置具有数万台设备的工业网络，包

括与安全相关的领域。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跨站脚本检索敏感信息，允许经过身份验证的低权限用户实现权限提升，使用 root 权限在设备上执行任意代码等。

CNVD 收录的相关漏洞包括：Siemens Polarion ALM 跨站脚本漏洞、Siemens SINUMERIK MC 权限提升漏洞、Siemens RUGGEDCOM ROS 堆缓冲区溢出漏洞、Siemens RUGGEDCOM ROS 整数溢出漏洞、Siemens RUGGEDCOM ROS 跨站脚本漏洞、Siemens SINEC NMS 反序列化漏洞、Siemens SINEC NMS 权限提升漏洞、Siemens SINEC NMS SQL 注入漏洞（CNVD-2022-17792）。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-2022-17778
https://www.cnvd.org.cn/flaw/show/CNVD-2022-17780
https://www.cnvd.org.cn/flaw/show/CNVD-2022-17783
https://www.cnvd.org.cn/flaw/show/CNVD-2022-17782
https://www.cnvd.org.cn/flaw/show/CNVD-2022-17786
https://www.cnvd.org.cn/flaw/show/CNVD-2022-17791
https://www.cnvd.org.cn/flaw/show/CNVD-2022-17790
https://www.cnvd.org.cn/flaw/show/CNVD-2022-17792

4、DELL 产品安全漏洞

Dell Vnx2 Oe For File 是美国戴尔（Dell）公司的一个操作环境。DELL EMC Integrated System 是美国戴尔（DELL）公司的一个本地混合云平台，用于提供基础架构和平台即服务。Dell Wyse Management Suite 是美国戴尔（DELL）公司的一套用于管理和优化 Wyse 端点的、可扩展的解决方案。该产品包括 Wyse 端点集中管理、资产追踪和自动设备发现等功能。DELL Dell Hybrid Client 是美国戴尔（DELL）公司的一个应用软件。提供一个具有混合云管理功能的客户端计算软件。Dell PowerScale OneFS 是美国 Dell 公司的一个操作系统。提供横向扩展 NAS 的 PowerScale OneFS 操作系统。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞获取日志信息，发送一个特殊的请求并在目标系统上执行任意代码，提升特权并接管系统等。

CNVD 收录的相关漏洞包括：Dell Vnx2 Oe For File 安全特征问题漏洞、Dell EMC Integrated System 权限提升漏洞、Dell VNX2 OE for File 敏感信息泄露漏洞、Dell Vnx2 Oe For File 操作系统命令注入漏洞、Dell Wyse Management Suite 反序列化漏洞、Dell Hybrid Client 访问控制错误漏洞、Dell PowerScale OneFS 访问控制错误漏洞、Dell Technologies Dell PowerScale OneFS 身份验证绕过漏洞。除“Dell VNX2 OE for File 敏感信息泄露漏洞、Dell PowerScale OneFS 访问控制错误漏洞、Dell Technologies Dell PowerScale OneFS 身份验证绕过漏洞”外漏洞的综合评级为“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-2022-18261
https://www.cnvd.org.cn/flaw/show/CNVD-2022-18266
https://www.cnvd.org.cn/flaw/show/CNVD-2022-18265
https://www.cnvd.org.cn/flaw/show/CNVD-2022-18264
https://www.cnvd.org.cn/flaw/show/CNVD-2022-18270
https://www.cnvd.org.cn/flaw/show/CNVD-2022-18275
https://www.cnvd.org.cn/flaw/show/CNVD-2022-18274
https://www.cnvd.org.cn/flaw/show/CNVD-2022-18272

5、Pybbs 跨站脚本漏洞

Pybbs 是一个更实用的 Java 开发的社区（论坛）。本周，Pybbs 被披露存在跨站脚本漏洞。攻击者可利用该漏洞执行客户端代码。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-2022-18013

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-2022-17103	TOTOLink T10 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://www.totolink.net/home/menu/detail/menu_listtpl/download/id/172/ids/36.html
CNVD-2022-17107	TOTOLink A3000RU 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://cxsecurity.com/cveshow/CVE-2022-25075/
CNVD-2022-17105	TOTOLink T6 命令注入漏洞（CNVD-2022-17105）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/EPhaha/IOT_vuln/blob/main/TOTOLink/T6/README.md
CNVD-2022-17111	TOTOLink A800R 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://github.com/EPhaha/IOT_vuln/blob/main/TOTOLink/A800R/README.md

CNVD-2022-17109	TOTOLink A860R 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://github.com/EPhaha/IOT_vuln/blob/main/TOTOLink/A860R/README.md
CNVD-2022-17108	TOTOLink A3600R 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://github.com/EPhaha/IOT_vuln/blob/main/TOTOLink/A3600R/README.md
CNVD-2022-17125	多款 TOTOLink 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，补丁获取链接：https://github.com/pjqwudi/my_vuln/blob/main/totolink/vuln_1/1.md
CNVD-2022-17766	Tp-link TL-WR840N 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：http://tp-link.com
CNVD-2022-18221	Libmobi 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://github.com/bfabiszewski/libmobi/commit/ab5bf0e37e540eac682a14e628853b918626e72b
CNVD-2022-18420	Nextcloud 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://github.com/nextcloud/security-advisories/security/advisories/GHSA-m682-v4g9-wrq7

小结：本周，Huawei 产品被披露存在多个漏洞，攻击者可利用漏洞导致随机地址访问，导致内核死机，将特制数据传递给应用程序并在目标系统上执行任意命令等。此外，Oracle、Siemens、DELL 等多款产品被披露存在多个漏洞，攻击者可利用漏洞跨站脚本检索敏感信息，允许经过身份验证的低权限用户实现权限提升，使用 root 权限在设备上执行任意代码等。另外，Pybbs 被披露存在跨站脚本漏洞。攻击者可利用该漏洞执行客户端代码。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、TOTOLink A830R 命令注入漏洞

验证描述

TOTOLink A830R 是中国 TotoLink 公司的一款无线双频路由器。

TOTOLink A830R V5.9c.4729_B20191112 版本存在命令注入漏洞，攻击者可利用

该漏洞通过 QUERY_STRING 参数执行任意命令。

验证信息

POC 链接：https://github.com/EPhaha/IOT_vuln/blob/main/TOTOLink/A830R/README.md

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2022-17104

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. 轮胎公司普利斯通美洲证实了勒索软件攻击，LockBit 泄露数据

LockBit 勒索软件团伙声称，对世界上最大的轮胎制造商之一普利斯通美洲公司(Bridgestone Americas)发起了网络攻击，并泄露了其数据。

参考链接：https://www.bleepingcomputer.com/news/security/bridgestone-americas-confirms-ransomware-attack-lockbit-leaks-data/

2. 僵尸网络 Emotet 卷土重来，已感染 179 个国家的 13 万台设备

Emotet 自去年 11 月复出以来发展迅速，已经感染了约 13 万台主机，遍布 179 个国家。

参考链接：https://www.freebuf.com/news/324520.html

关于 CNVD

国家信息安全漏洞共享平台（China National Vulnerability Database，简称 CNVD）是 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信息安全漏洞信息共享知识库，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，是我国网络安全应急体系的核心协调机构。

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