国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2022 年 04 月 04 日-2022 年 04 月 10 日 **2022 年第 14 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 160 个，其中高危漏洞 65 个、中危漏洞 78 个、低危漏洞 17 个。漏洞平均分值为 6.17。本周收录的漏洞中，涉及 0day 漏洞 97 个（占 61%），其中互联网上出现“Apache James Server 远程命令执行漏洞、WordPress 插件 Wappointment 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事件型漏洞总数 3611 个，与上周（5300 个）环比减少 32%。

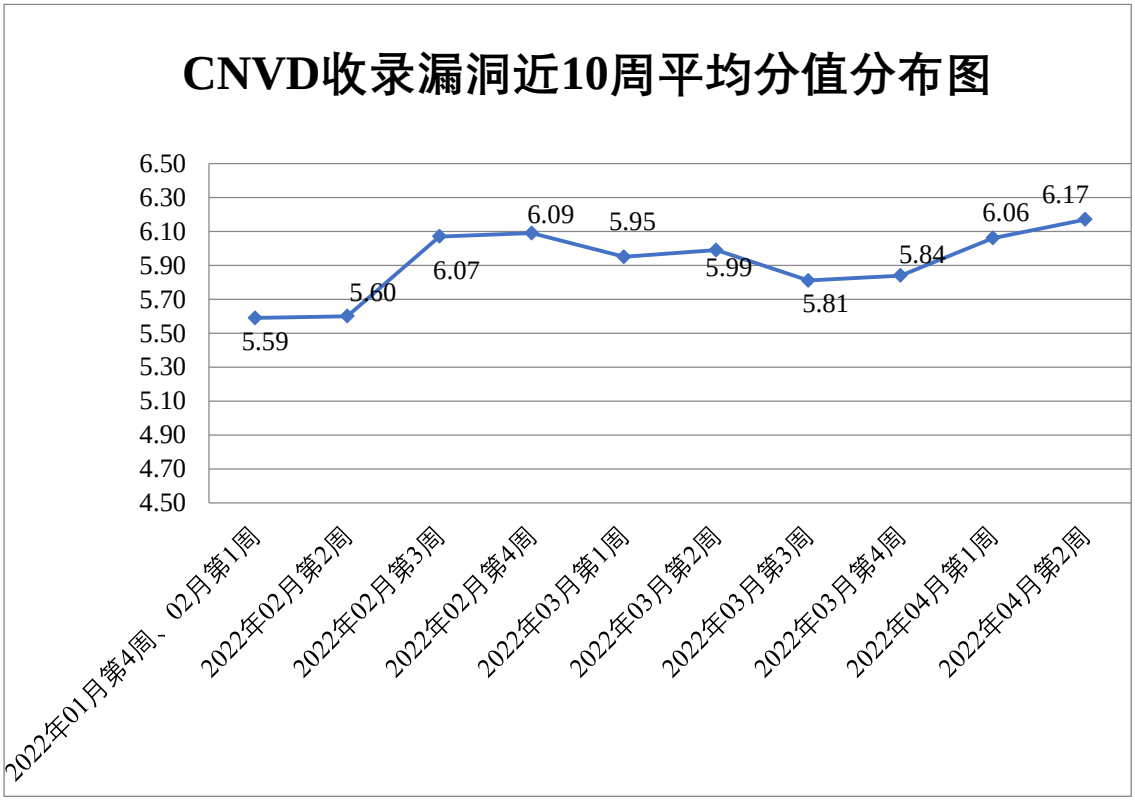

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 27 起，向基础电信企业通报漏洞事件 40 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 149 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 48 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 94 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：

淄博闪灵网络科技有限公司、友讯电子设备（上海）有限公司、兄弟（中国）商业有限公司、微软（中国）有限公司、四川迅睿云软件开发有限公司、四川蜀天梦图数据科技有限公司、深圳市远望谷信息技术股份有限公司、深圳市吉祥腾达科技有限公司、深圳市必联电子有限公司、深圳市安网科技有限公司、上海卓卓网络科技有限公司、上海穆云智能科技有限公司、上海宽尔网络科技有限公司、上海泛微网络科技股份有限公司、熵基科技股份有限公司、山东渔翁信息技术股份有限公司、厦门优优汇联信息科技股份有限公司、三星（中国）投资有限公司、青岛和晟思壮测控技术有限公司、蚂蚁金服（杭州）网络技术有限公司、廊坊市极致网络科技有限公司、居易科技股份有限公司、江西铭软科技有限公司、江苏群立现代信息科技发展有限公司、惠普贸易（上海）有限公司、杭州海康威视数字技术股份有限公司、桂林崇胜网络科技有限公司、帆软软件有限公司、东芝（中国）有限公司、点都软件（上海）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、北京五指互联科技有限公司、北京书生电子技术有限公司、北京坤豆科技有限公司、北京九思协同软件有限公司、北京金万维科技有限公司、北京谷翔信息技术有限公司、北京东方通科技股份有限公司、北京百卓网络技术有限公司、网展科技、阿里巴巴集团安全应急响应中心、梦想 cms 、ZZZCMS、YIXUNCMS、VACRON、TRENDnet、seacms、NetSarang、MacCMS、KEO、Grafana Labs、EasyGoAdmin 和 Apache。

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、深信服科技股份有限公司、厦门服云信息科技有限公司、杭州安恒信息技术股份有限公司、安天科技集团股份有限公司等单位报送公开收集的漏洞数量较多。重庆都会信息科技有限公司、北京山石网科信息技术有限公司、贵州泰若数字科技有限公司、杭州默安科技有限公司、江苏保旺达软件技术有限公司、星云博创科技有限公司、内蒙古洞明科技有限公司、武汉安域信息安全技术有限公司、任子行网络技术股份有限公司、河南信安世纪科技有限公司、长春

嘉诚信息技术股份有限公司、山东云天安全技术有限公司、快页信息技术有限公司、广州百蕴启辰科技有限公司、北方实验室（沈阳）股份有限公司、南京节点安全技术有限公司、上海嘉韦思信息技术有限公司、墨菲未来科技（北京）有限公司、麒麟软件有限公司、有度网络安全技术有限公司、上海纽盾科技股份有限公司、上海上讯信息技术股份有限公司、北京天地和兴科技有限公司、南京禾盾信息科技有限公司、厦门捷诺通信息技术股份有限公司、山东泽鹿安全技术有限公司、广州安亿信软件科技有限公司、四川赛闯检测股份有限公司、河北华测信息技术有限公司、博智安全科技股份有限公司及其他个人白帽子向 CNVD 提交了 3611 个以事件型漏洞为主的原创漏洞，其中包括上海交大、斗象科技（漏洞盒子）和奇安信网神（补天平台）向 CNVD 共享的白帽子报送的 1354 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
上海交大	836	836
斗象科技（漏洞盒子）	426	426
新华三技术有限公司	251	0
深信服科技股份有限公司	218	0
厦门服云信息科技有限公司	198	0
杭州安恒信息技术股份有限公司	154	20
安天科技集团股份有限公司	140	0
北京天融信网络安全技术有限公司	119	20
恒安嘉新（北京）科技股份公司	100	0
北京启明星辰信息安全技术有限公司	93	29
奇安信网神（补天平台）	92	92
西安四叶草信息技术有限公司	87	87
天津市国瑞数码安全	59	0

系统股份有限公司		
北京神州绿盟科技有限公司	56	1
三六零数字安全科技集团有限公司	52	0
中国电信集团系统集成有限责任公司	30	0
北京数字观星科技有限公司	28	0
内蒙古云科数据服务股份有限公司	17	17
京东科技信息技术有限公司	11	11
北京安信天行科技有限公司	1	1
北京知道创宇信息技术有限公司	1	1
北京华顺信安科技有限公司	260	0
重庆都会信息科技有限公司	130	130
亚信科技（成都）有限公司	48	0
北京山石网科信息技术有限公司	20	20
贵州泰若数字科技有限公司	13	13
杭州默安科技有限公司	13	13
江苏保旺达软件技术有限公司	12	12
杭州迪普科技股份有限公司	11	0
星云博创科技有限公	11	11

司		
内蒙古洞明科技有限公司	10	10
武汉安域信息安全技术有限公司	8	8
任子行网络技术股份有限公司	5	5
河南信安世纪科技有限公司	5	5
长春嘉诚信息技术股份有限公司	5	5
山东云天安全技术有限公司	4	4
快页信息技术有限公司	4	4
广州百蕴启辰科技有限公司	3	3
北方实验室（沈阳）股份有限公司	2	2
南京节点安全技术有限公司	2	2
上海嘉韦思信息技术有限公司	2	2
墨菲未来科技（北京）有限公司	2	2
麒麟软件有限公司	1	1
有度网络安全技术有限公司	1	1
上海纽盾科技股份有限公司	1	1
上海上讯信息技术股份有限公司	1	1
北京天地和兴科技有限公司	1	1

南京禾盾信息科技有限公司	1	1
厦门捷诺通信息技术股份有限公司	1	1
山东泽鹿安全技术有限公司	1	1
广州安亿信软件科技有限公司	1	1
四川赛闯检测股份有限公司	1	1
河北华测信息技术有限公司	1	1
博智安全科技股份有限公司	1	1
CNCERT 四川分中心	5	5
CNCERT 河北分中心	2	2
个人	1800	1800
报送总计	5358	3611

本周漏洞按类型和厂商统计

本周，CNVD 收录了 160 个漏洞。WEB 应用 76 个，应用程序 27 个，网络设备（交换机、路由器等网络端设备）23 个，操作系统 23 个，智能设备（物联网终端设备）8 个，安全产品 2 个，数据库 1 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	76
应用程序	27
网络设备（交换机、路由器等网络端设备）	23
操作系统	23
智能设备（物联网终端设备）	8
安全产品	2
数据库	1

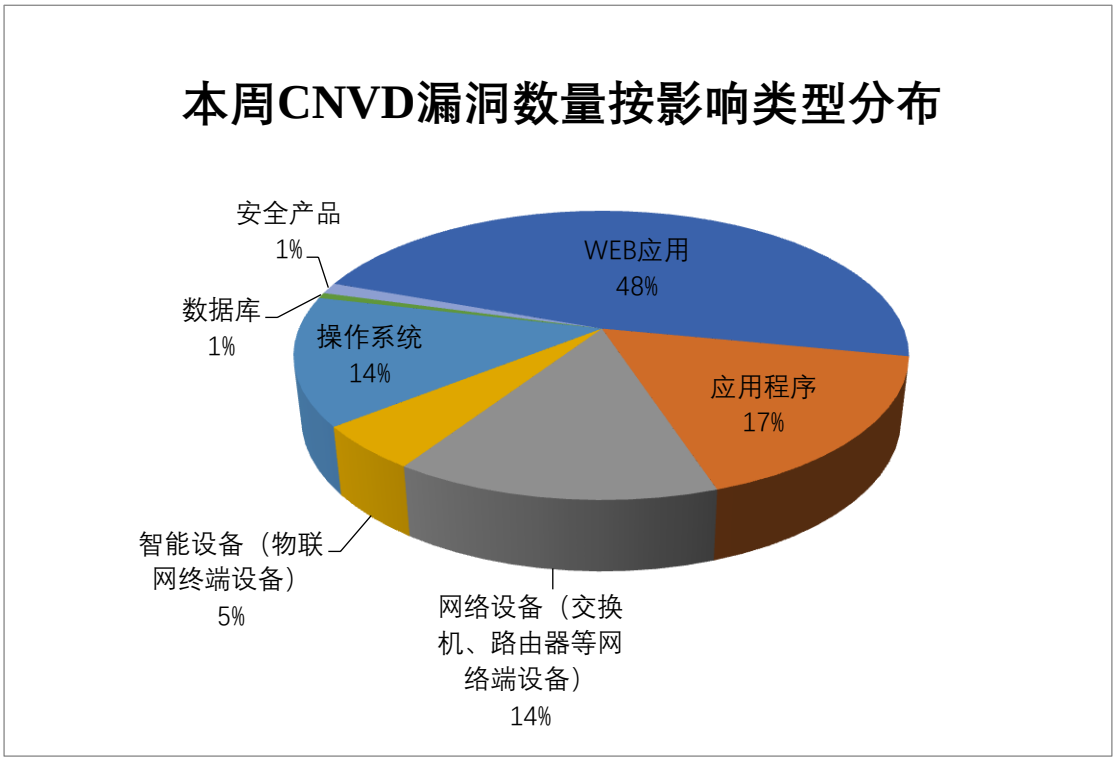

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Google、F5、Delta Electronics 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	Google	20	13%
2	F5	12	8%
3	Delta Electronics	11	7%
4	Tenda	10	6%
5	WordPress	9	6%
6	TOTOLINK	7	4%
7	Adobe	7	4%
8	Brickcom	5	3%
9	北京万维盈创科技发展有限公司	4	3%
10	其他	75	46%

本周行业漏洞收录情况

本周，CNVD 收录了 21 个电信行业漏洞，22 个移动互联网行业漏洞，1 个工控行业漏洞（如下图所示）。其中，“Tenda AC6 缓冲区溢出漏洞、Google Android 权限提升漏洞（CNVD-2022-26766）”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/

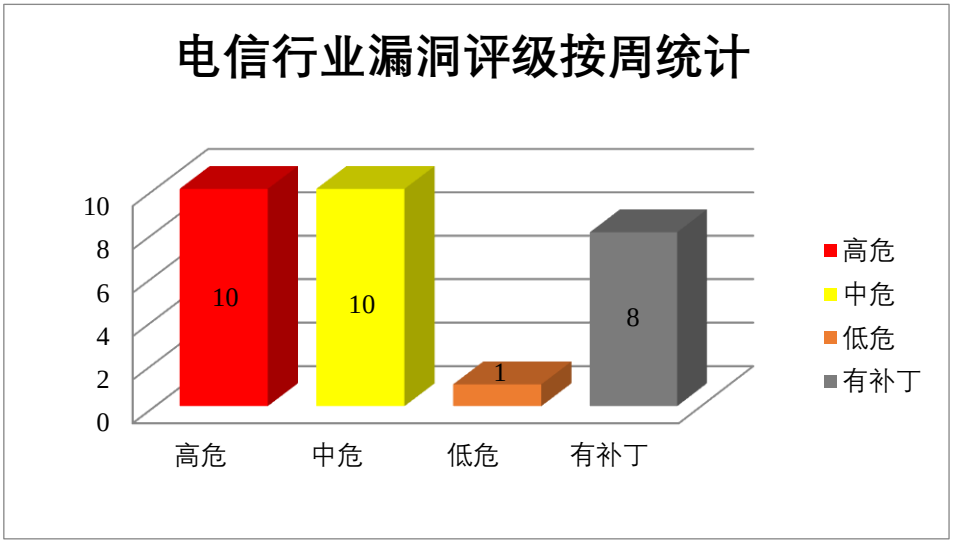

图 3 电信行业漏洞统计

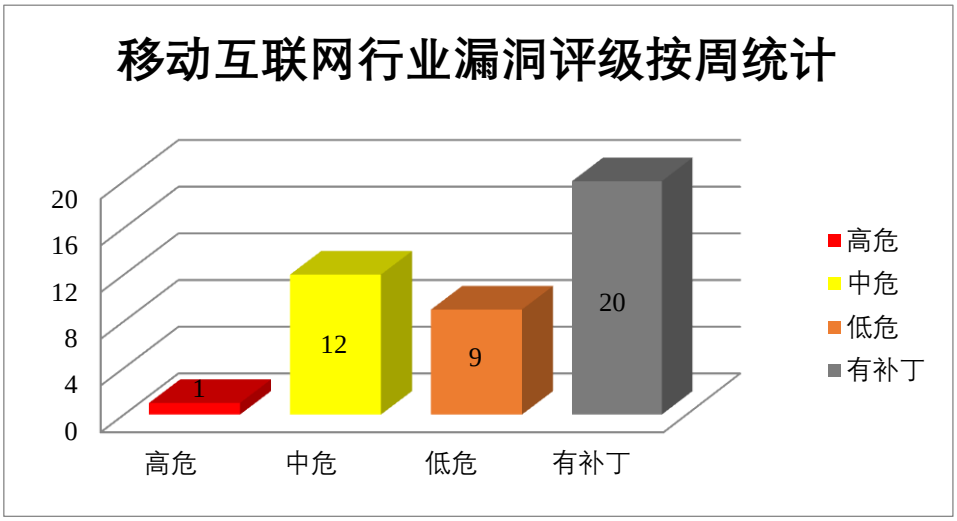

图 4 移动互联网行业漏洞统计

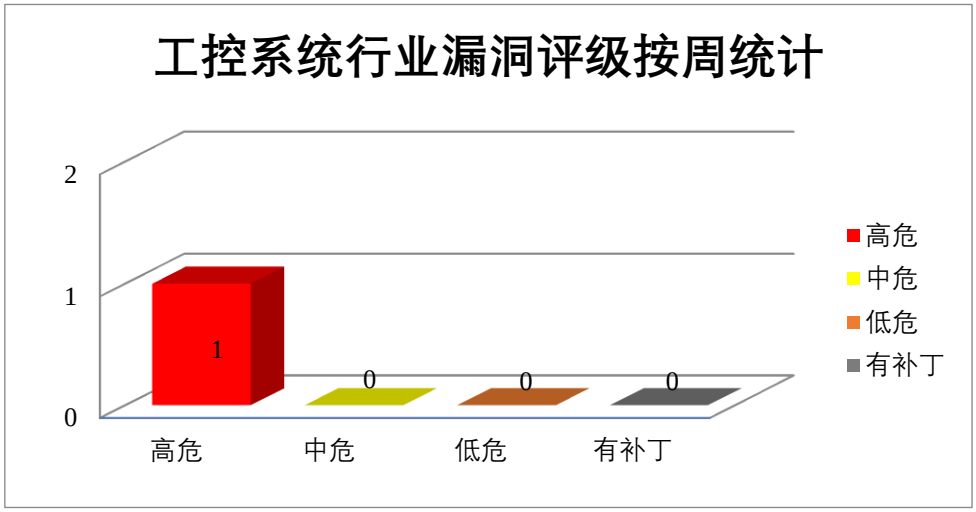

图 5 工控系统行业漏洞统计

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 Android 是美国谷歌（Google）公司的的一套以 Linux 为基础的开源操作系统。本周，上述产品被披露存在权限提升漏洞，攻击者可利用漏洞升级权限。

CNVD 收录的相关漏洞包括：Google Android 权限提升漏洞（CNVD-2022-26764、CNVD-2022-26762、CNVD-2022-26761、CNVD-2022-26766、CNVD-2022-26765、CNVD-2022-26773、CNVD-2022-26771、CNVD-2022-26782）。其中，“Google Android 权限提升漏洞（CNVD-2022-26766）”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-2022-26764

https://www.cnvd.org.cn/flaw/show/CNVD-2022-26762

https://www.cnvd.org.cn/flaw/show/CNVD-2022-26761

https://www.cnvd.org.cn/flaw/show/CNVD-2022-26766

https://www.cnvd.org.cn/flaw/show/CNVD-2022-26765

https://www.cnvd.org.cn/flaw/show/CNVD-2022-26773

https://www.cnvd.org.cn/flaw/show/CNVD-2022-26771

https://www.cnvd.org.cn/flaw/show/CNVD-2022-26782

2、F5 产品安全漏洞

F5 BIG-IP 是美国 F5 公司的一款集成了网络流量管理、应用程序安全管理、负载均衡等功能的应用交付平台。F5 BIG-IQ 是美国 F5 公司的一套基于软件的云管理解决

方案。该方案支持跨公共和私有云、传统数据中心和混合环境部署应用交付和网络服务。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞提升权限，执行未经授权的操作，导致拒绝服务等。

CNVD 收录的相关漏洞包括：F5 BIG-IP 跨站脚本漏洞（CNVD-2022-26776、CNVD-2022-26778）、F5 BIG-IP 输入验证错误漏洞（CNVD-2022-26839、CNVD-2022-26779）、F5 BIG-IP 命令注入漏洞（CNVD-2022-26777）、F5 BIG-IQ 访问控制错误漏洞（CNVD-2022-26842）、F5 BIG-IP APM 输入验证错误漏洞（CNVD-2022-26841）、F5 BIG-IP 授权问题漏洞（CNVD-2022-26845）。其中，“F5 BIG-IQ 访问控制错误漏洞（CNVD-2022-26842）”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-2022-26776
https://www.cnvd.org.cn/flaw/show/CNVD-2022-26778
https://www.cnvd.org.cn/flaw/show/CNVD-2022-26839
https://www.cnvd.org.cn/flaw/show/CNVD-2022-26779
https://www.cnvd.org.cn/flaw/show/CNVD-2022-26777
https://www.cnvd.org.cn/flaw/show/CNVD-2022-26842
https://www.cnvd.org.cn/flaw/show/CNVD-2022-26841
https://www.cnvd.org.cn/flaw/show/CNVD-2022-26845

3、Tenda 产品安全漏洞

Tenda AC9 是中国腾达（Tenda）公司的一款无线路由器。本周，上述产品被披露存在命令注入和缓冲区溢出漏洞，攻击者可利用漏洞导致任意命令执行。

CNVD 收录的相关漏洞包括：Tenda AC9 命令注入漏洞（CNVD-2022-26241、CNVD-2022-26245）、Tenda AC9 缓冲区溢出漏洞（CNVD-2022-26244、CNVD-2022-26243、CNVD-2022-26242、CNVD-2022-26246、CNVD-2022-26247）、Tenda AC6 缓冲区溢出漏洞。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-2022-26241
https://www.cnvd.org.cn/flaw/show/CNVD-2022-26245
https://www.cnvd.org.cn/flaw/show/CNVD-2022-26244
https://www.cnvd.org.cn/flaw/show/CNVD-2022-26243
https://www.cnvd.org.cn/flaw/show/CNVD-2022-26242
https://www.cnvd.org.cn/flaw/show/CNVD-2022-26246
https://www.cnvd.org.cn/flaw/show/CNVD-2022-26247
https://www.cnvd.org.cn/flaw/show/CNVD-2022-26249

4、Delta Electronics 产品安全漏洞

Delta Electronics DIAEnergie 是一个工业能源管理系统，用于实时监控和分析能源消耗、计算能源消耗和负载特性、优化设备性能、改进生产流程并最大限度地提高能源效率。本周，上述产品被披露存在 SQL 注入漏洞，攻击者可利用漏洞注入任意 SQL 查询、检索和修改数据库内容以及执行系统命令。

CNVD 收录的相关漏洞包括：Delta Electronics DIAEnergie SQL 注入漏洞（CNVD-2022-27435、CNVD-2022-27434、CNVD-2022-27438、CNVD-2022-27437、CNVD-2022-27436、CNVD-2022-27441、CNVD-2022-27440、CNVD-2022-27439）。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-2022-27435

https://www.cnvd.org.cn/flaw/show/CNVD-2022-27434

https://www.cnvd.org.cn/flaw/show/CNVD-2022-27438

https://www.cnvd.org.cn/flaw/show/CNVD-2022-27437

https://www.cnvd.org.cn/flaw/show/CNVD-2022-27436

https://www.cnvd.org.cn/flaw/show/CNVD-2022-27441

https://www.cnvd.org.cn/flaw/show/CNVD-2022-27440

https://www.cnvd.org.cn/flaw/show/CNVD-2022-27439

5、Reolink Rlc-410W 拒绝服务漏洞（CNVD-2022-27432）

Reolink Rlc-410W 是中国 Reolink 公司的一款 Wifi 安全摄像头。本周，Reolink RLC-410W 存在拒绝服务漏洞。攻击者可利用漏洞通过编制的 HTTP 请求，导致重新启动。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-2022-27432

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-2022-26243	Tenda AC9 缓冲区溢出漏洞（CNVD-2022-26243）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.tenda.com.cn/download/cata-11.html
CNVD-2022-27443	Delta Electronics DIAEnergie 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.deltaww.com/en-US/index
CNVD-2022-27444	Synology DiskStation Manager SQL 注入漏洞（CNVD-2022-27444）	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.synology.com
CNVD-2022-	Tenda AC6 缓冲区溢	高	厂商已发布了漏洞修复程序，请及时关

26249	出漏洞		注更新：https://www.tenda.com.cn/download/cata-11.html
CNVD-2022-26766	Google Android 权限提升漏洞（CNVD-2022-26766）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://source.android.com/security/bulletin/android-12l
CNVD-2022-27445	Synology DiskStation Manager SQL 注入漏洞（CNVD-2022-27445）	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.synology.com
CNVD-2022-26842	F5 BIG-IQ 访问控制错误漏洞（CNVD-2022-26842）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://support.f5.com/csp/article/K40084114
CNVD-2022-27442	Delta Electronics DIAEnergie SQL 注入漏洞（CNVD-2022-27442）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.deltaww.com/
CNVD-2022-26247	Tenda AC9 缓冲区溢出漏洞（CNVD-2022-26247）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.tenda.com.cn/download/cata-11.html
CNVD-2022-27446	Synology DiskStation Manager SQL 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.synology.com

小结：本周，Google 产品被披露存在权限提升漏洞，攻击者可利用漏洞升级权限。此外，F5、Tenda、Delta Electronics 等多款产品被披露存在多个漏洞，攻击者可利用漏洞执行未经授权的操作，注入任意 SQL 查询、检索和修改数据库内容以及执行系统命令，导致拒绝服务等。另外，Reolink Rlc-410W 被披露存在拒绝服务漏洞，攻击者可利用漏洞通过编制的 HTTP 请求，导致重新启动。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、Apache James Server 远程命令执行漏洞

验证描述

Apache James Server 是美国阿帕奇（Apache）软件基金会的一款采用纯 Java 技术开发的开源 SMTP 和 POP3 邮件服务器及 NNTP 新闻服务器。

Apache James Server 存在远程命令执行漏洞。攻击者可利用该漏洞在浏览器上下文中执行任意代码。

验证信息

POC 链接：https://cxsecurity.com/issue/WLB-2021090142

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2022-27430

信息提供者

深信服科技股份有限公司

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. GitLab 高危漏洞允许攻击者控制用户账号

GitLab 修复了一个高危漏洞，该漏洞影响 GitLab Community Edition (CE)和 Enterprise Edition (EE)，允许远程攻击者使用硬编码密码控制用户账号。

参考链接：https://www.solidot.org/story?sid=71140

2. Microsoft Azure Automation 被发现高危的账户越权访问漏洞

AutoWarp 是 Azure 自动化服务中的一个关键漏洞，它允许未经授权的用户访问使用该服务的其他 Azure 客户帐户。这种攻击可能意味着完全控制属于目标帐户的资源和数据，具体取决于客户分配的权限。

参考链接：https://www.4hou.com/posts/WoVQ

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