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 25 日-2022 年 05 月 08 日　　2022 年第 17、18 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 603 个，其中高危漏洞 189 个、中危漏洞 345 个、低危漏洞 69 个。漏洞平均分值为 5.92。本周收录的漏洞中，涉及 0day 漏洞 412 个（占 68%），其中互联网上出现“Tenda M3 命令注入漏洞（CNVD-2022-33113）、MariaDB item_subselect.cc 拒绝服务漏洞”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 14613 个，与上周（9337 个）环比增加 57%。

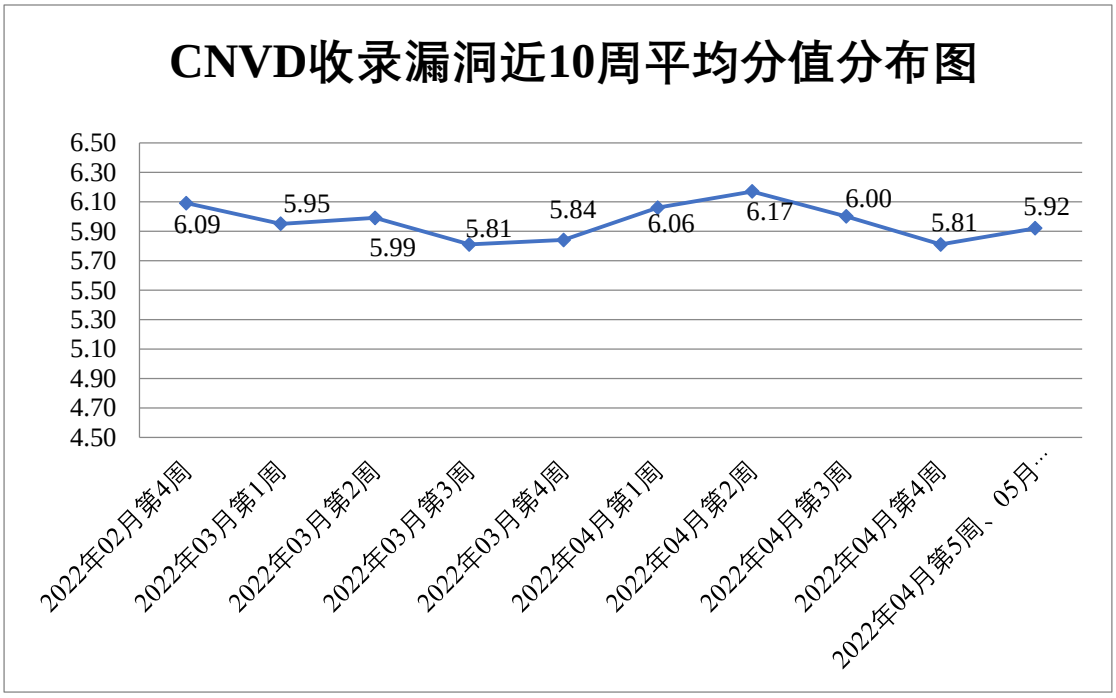

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 80 起，向基础电

信企业通报漏洞事件 82 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 1390 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 211 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 232 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、珠海奥威软件科技有限公司、重庆旱獭信息技术有限公司、郑州畅威物联网科技有限公司、正方软件股份有限公司、浙江自贸区耀光网络科技有限公司、浙江臻善科技股份有限公司、浙江宇视科技有限公司、浙江大华技术股份有限公司、长沙云川信息技术有限公司、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、易赴科技（集团）有限公司、义乌中国小商品城大数据有限公司、兄弟（中国）商业有限公司、西门子（中国）有限公司、西安知先信息技术公司、西安九佳易信息资讯有限公司、武汉金同方科技有限公司、无锡信捷电气股份有限公司、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、腾讯安全应急响应中心、太原迅易科技有限公司、苏州科达科技股份有限公司、苏州恩斯特网络科技有限公司、四平市九州易通科技有限公司、四创科技有限公司、思科系统（中国）网络技术有限公司、思创数码科技股份有限公司、深圳众为兴技术股份有限公司、深圳市万网博通科技有限公司、深圳市四海众联网络科技有限公司、深圳市吉祥腾达科技有限公司、深圳市汇川技术股份有限公司、深圳市必联电子有限公司、深圳市艾米通信有限公司、深圳前海华夏智信数据科技有限公司、深圳伴生活科技有限公司、上海卓卓网络科技有限公司、上海新时达电气股份有限公司、上海携宁计算机科技股份有限公司、上海牛之云科技有限公司、上海穆云智能科技有限公司、上海劳勤信息技术有限公司、上海华测导航技术股份有限公司、上海富数科技有限公司、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、上海二三四五移动科技有限公司、熵基科技股份有限公司、山东博硕自动化技术有限公司、厦门宇能科技有限公司、厦门一指通智能科技有限公司、厦门四信通信科技有限公司、厦门市灵鹿谷科技有限公司、三星（中国）投资有限公司、润申信息科技（上海）有限公司、睿易教育科技股份有限公司、千百万信用评估有限公司、普联软件股份有限公司、普联技术有限公司、宁波中茂网络科技有限公司、宁波一威信息科技有限公司、南京南软科技有限公司、茉柏枘（上海）软件科技有限公司、美国谷歌（Google）公司、昂氏（上海）电子贸易有限公司、理光（中国）投资有限公司、乐视网信息技术（北京）股份有限公司、敬业钢铁有限公司、景安大数据科技有限公司、京火星高科数字科技有限公司、金蝶软件（中国）有限公司、江苏汇文软件有限公司、佳能（中国）有限公司、吉翁电子（深圳）有限公司、惠普贸易（上海）有限公司、湖南壹拾捌号网络技术有限公司、恒锋信息科技股份有限公司、河北先河环保科技股份有限公司、杭州可道云网络有限公司、杭州迪普科技

股份有限公司、海南有趣科技有限公司、海纳医信（北京）软件科技有限责任公司、广州市凝智科技有限公司、广州市保伦电子有限公司、广州红帆科技有限公司、广州和丰自动化科技有限公司、广州富宏智能科技有限公司、广西南宁领众网络科技有限公司、福建银达汇智信息科技股份有限公司、福建福昕软件开发股份有限公司、飞利浦（中国）投资有限公司、帆软软件有限公司、东莞市智跃软件科技有限公司、东莞市彭氏智能科技有限公司、成都中科大旗软件股份有限公司、成都乐云互动网络技术有限公司、畅捷通信息技术股份有限公司、贝尔金国际有限公司、北京中文在线文化传媒有限公司、北京中庆现代技术股份有限公司、北京智邦国际软件技术有限公司、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、北京小米科技有限责任公司、北京五指互联科技有限公司、北京网康科技有限公司、北京通达信科科技有限公司、北京神州数码云科信息技术有限公司、北京旗硕基业科技股份有限公司、北京酷我科技有限公司、北京九思协同软件有限公司、北京慧图科技（集团）股份有限公司、北京国炬信息技术有限公司、北京博海琪林科技有限公司、北京宝兰德软件股份有限公司、百度安全应急响应中心、安徽旭帆信息科技有限公司、阿里巴巴集团安全应急响应中心、若依、龙蜥开源社区、勾股 CMS、大米 CMS、zzzcms、ZZCMS、VoIP Group、The Apache Software Foundation、snowy-layui、ShirneCMS、Resort Reservation System、PHPEMS、Oracle、NexusQA、Jfinal cms、Internship Portal Management System、Gadget Works Online Ordering System、Axis Communications AB、Avatar、Adobe 和 A10 Networks。

本周，CNVD 发布了《关于 F5 BIG-IP iControl REST 存在身份认证绕过漏洞的安全公告》。详情参见 CNVD 网站公告内容。

https://www.cnvd.org.cn/webinfo/show/7656

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、杭州安恒信息技术股份有限公司、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、内蒙古洞明科技有限公司、重庆都会信息科技有限公司、武汉安域信息安全技术有限公司、杭州迪普科技股份有限公司、长春嘉诚信息技术股份有限公司、星云博创科技有限公司、上海纽盾科技股份有限公司、河南信安世纪科技有限公司、南京树安信息技术有限公司、山东云天安全技术有限公司、河南灵创电子科技有限公司、杭州默安科技有限公司、快页信息技术有限公司、华鲁数智信息技术（北京）有限公司、江苏保旺达软件技术有限公司、北京山石网科信息技术有限公司、深圳昂楷科技有限公司、广西等保安全测评有限公司、智网安云（武汉）信息技术有限公司、河南省鼎信信息安全等级测评有限公司、北京机沃科技有限公司、山石网科通信技术股份有限公司、任子行网络技术股份有限公

司、巨鹏信息科技有限公司、湖北珞格科技发展有限公司、西藏熙安信息技术有限责任公司、西安交大捷普网络科技有限公司、深圳市魔方安全科技有限公司、上海嘉韦思信息技术有限公司、麒麟软件有限公司、平安银河实验室、南京节点安全技术有限公司、黑龙江亿林网络股份有限公司、杭州海康威视数字技术股份有限公司、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、广西塔易信息技术有限公司、北京威努特技术有限公司、北京惠而特科技有限公司、北京国测信安科技有限公司、北方实验室（沈阳）股份有限公司及其他个人白帽子向 CNVD 提交了 14613 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 10503 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）	4283	4283
奇安信网神（补天平台）	4245	4245
上海交大	1975	1975
深信服科技股份有限公司	1002	0
杭州安恒信息技术股份有限公司	729	148
新华三技术有限公司	406	0
安天科技集团股份有限公司	346	0
三六零数字安全科技集团有限公司	340	340
北京天融信网络安全技术有限公司	293	26
北京神州绿盟科技有限公司	280	9
北京数字观星科技有限公司	271	0
恒安嘉新（北京）科技股份公司	185	0
天津市国瑞数码安	116	0

全系统股份有限公司		
北京启明星辰信息安全技术有限公司	65	8
西安四叶草信息技术有限公司	54	54
南京众智维信息科技有限公司	46	46
京东科技信息技术有限公司	40	4
中国电信集团系统集成有限责任公司	25	0
北京知道创宇信息技术有限公司	12	3
南京联成科技发展股份有限公司	12	12
内蒙古云科数据服务股份有限公司	7	7
远江盛邦（北京）网络安全科技股份有限公司	7	7
内蒙古奥创科技有限公司	5	5
北京安信天行科技有限公司	3	3
卫士通信息产业股份有限公司	3	3
深圳市腾讯计算机系统有限公司（玄武实验室）	1	1
北京华顺信安科技有限公司	560	0
贵州泰若数字科技有限公司	282	282
墨菲未来科技（北	97	0

京）有限公司		
内蒙古洞明科技有限公司	93	93
重庆都会信息科技有限公司	42	42
亚信科技（成都）有限公司	34	0
武汉安域信息安全技术有限公司	26	26
杭州迪普科技股份有限公司	26	1
长春嘉诚信息技术股份有限公司	25	25
星云博创科技有限公司	20	20
上海纽盾科技股份有限公司	20	20
河南信安世纪科技有限公司	18	18
南京树安信息技术有限公司	14	14
山东云天安全技术有限公司	13	13
河南灵创电子科技有限公司	8	8
杭州默安科技有限公司	8	8
快页信息技术有限公司	7	7
华鲁数智信息技术（北京）有限公司	7	7
江苏保旺达软件技术有限公司	6	6
北京山石网科信息技术有限公司	5	5

深圳昂楷科技有限公司	4	4
广西等保安全测评有限公司	4	4
智网安云（武汉）信息技术有限公司	3	3
河南省鼎信信息安全等级测评有限公司	3	3
北京机沃科技有限公司	3	3
山石网科通信技术股份有限公司	2	2
任子行网络技术股份有限公司	2	2
巨鹏信息科技有限公司	2	2
湖北珞格科技发展有限公司	2	2
西门子（中国）有限公司	1	0
西藏熙安信息技术有限责任公司	1	1
西安交大捷普网络科技有限公司	1	1
深圳市魔方安全科技有限公司	1	1
上海嘉韦思信息技术有限公司	1	1
麒麟软件有限公司	1	1
平安银河实验室	1	1
南京节点安全技术有限公司	1	1
黑龙江亿林网络股份有限公司	1	1

杭州海康威视数字技术股份有限公司	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
广西塔易信息技术有限公司	1	1
北京威努特技术有限公司	1	1
北京惠而特科技有限公司	1	1
北京国测信安科技有限公司	1	1
北方实验室（沈阳）股份有限公司	1	1
CNCERT 内蒙古分中心	3	3
CNCERT 河北分中心	1	1
CNCERT 贵州分中心	1	1
个人	2793	2793
报送总计	18902	14613

本周漏洞按类型和厂商统计

本周，CNVD 收录了 603 个漏洞。WEB 应用 277 个，应用程序 133 个，网络设备（交换机、路由器等网络端设备）81 个，数据库 42 个，操作系统 40 个，智能设备（物联网终端设备）28 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	277
应用程序	133
网络设备（交换机、路由器等网络端设备）	81
数据库	42

操作系统	40
智能设备（物联网终端设备）	28
安全产品	2

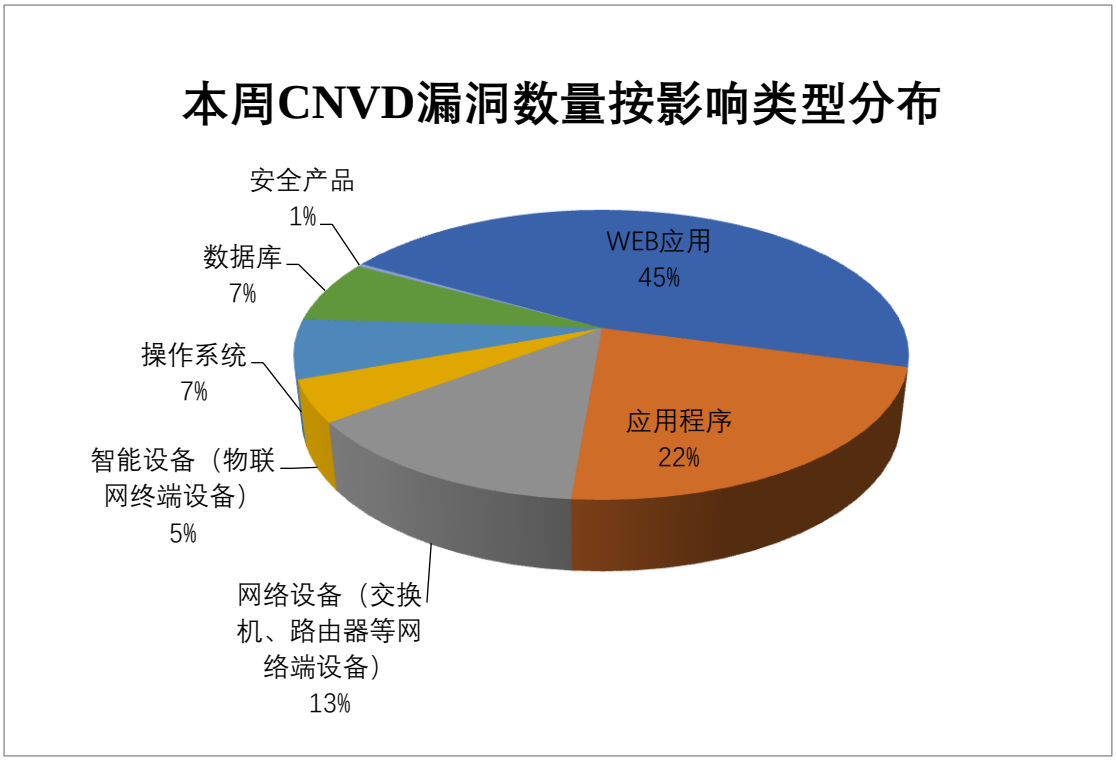

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 SourceCodester、Laurent Rineau、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	SourceCodester	43	7%
2	Laurent Rineau	31	5%
3	Tenda	26	5%
4	Oracle	25	5%
5	DELL	24	4%
6	Samsung	15	2%
7	Accusoft	14	2%
8	IBM	14	2%
9	FIS	14	2%
10	其他	397	66%

本周行业漏洞收录情况

本周，CNVD 收录了 67 个电信行业漏洞，28 个移动互联网行业漏洞（如下图所示）。

其中，“Xiaomi MIUI 权限提升漏洞、ASUS RT-AX88U 代码执行漏洞、Google Android TBD 权限提升漏洞”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/

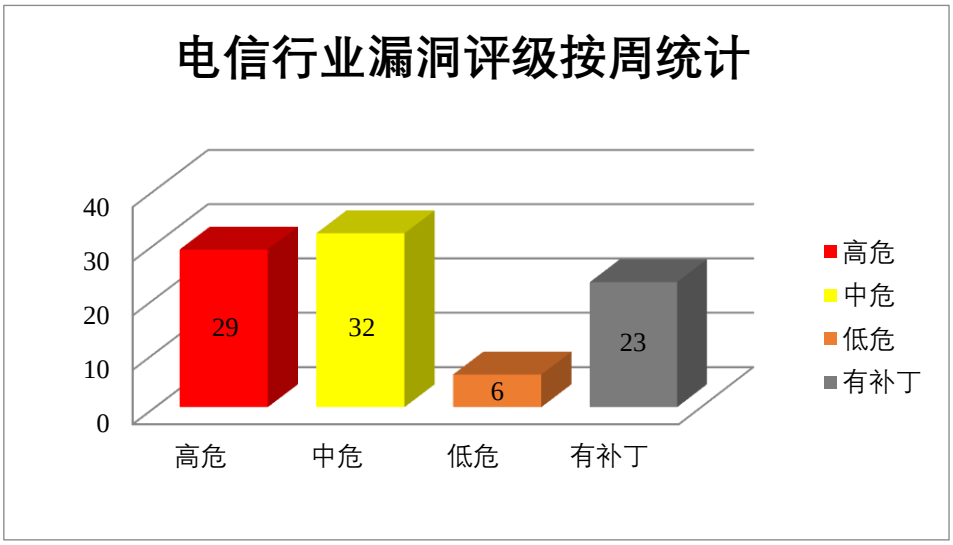

图 3 电信行业漏洞统计

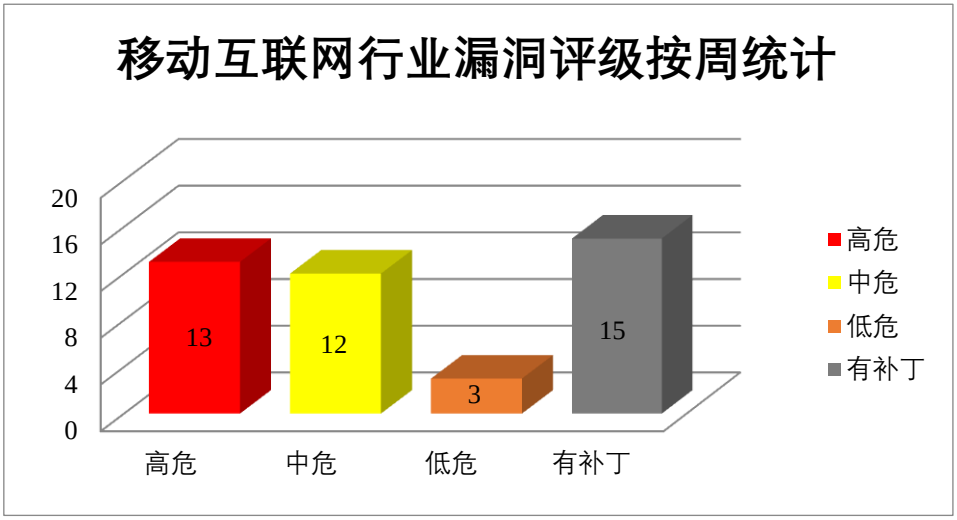

图 4 移动互联网行业漏洞统计

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多个漏洞，攻击者可利用漏洞获取敏感信息，任意修改和设置系统属性，升级权限等。

CNVD 收录的相关漏洞包括：Google Android 权限提升漏洞（CNVD-2022-32839、CNVD-2022-32843、CNVD-2022-32842、CNVD-2022-32844、CNVD-2022-34649）、Google Android 信息泄露漏洞（CNVD-2022-32846）、Google Android 安全绕过漏洞（CNVD-2022-32845）、Google Android TBD 权限提升漏洞。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-2022-32839
https://www.cnvd.org.cn/flaw/show/CNVD-2022-32843
https://www.cnvd.org.cn/flaw/show/CNVD-2022-32842
https://www.cnvd.org.cn/flaw/show/CNVD-2022-32846
https://www.cnvd.org.cn/flaw/show/CNVD-2022-32845
https://www.cnvd.org.cn/flaw/show/CNVD-2022-32844
https://www.cnvd.org.cn/flaw/show/CNVD-2022-34650
https://www.cnvd.org.cn/flaw/show/CNVD-2022-34649

2、 Oracle 产品安全漏洞

Oracle Fusion Middleware 是一套面向企业和云环境的业务创新平台。该平台提供了中间件、软件集合等功能。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 MySQL 是美国甲骨文（Oracle）公司的一套开源的关系数据库管理系统。MySQL Server 是其中的一个数据库服务器组件。MySQL Connectors 是其中的一个连接使用 MySQL 的应用程序的驱动程序。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞通过多种协议进行网络访问，从而破坏 MySQL Server，导致 MySQL Server 挂起或频繁崩溃（拒绝服务）等。

CNVD 收录的相关漏洞包括：Oracle Fusion Middleware 和 Oracle WebLogic Server 输入验证错误漏洞（CNVD-2022-33111）、Oracle MySQL 输入验证错误漏洞（CNVD-2022-33780、CNVD-2022-33779）、Oracle MySQL Server 拒绝服务漏洞（CNVD-2022-33991、CNVD-2022-33990、CNVD-2022-33992、CNVD-2022-33996、CNVD-2022-33995）。其中，“Oracle Fusion Middleware 和 Oracle WebLogic Server 输入验证错误漏洞（CNVD-2022-33111）”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-2022-33111
https://www.cnvd.org.cn/flaw/show/CNVD-2022-33780
https://www.cnvd.org.cn/flaw/show/CNVD-2022-33779

https://www.cnvd.org.cn/flaw/show/CNVD-2022-33991

https://www.cnvd.org.cn/flaw/show/CNVD-2022-33990

https://www.cnvd.org.cn/flaw/show/CNVD-2022-33992

https://www.cnvd.org.cn/flaw/show/CNVD-2022-33996

https://www.cnvd.org.cn/flaw/show/CNVD-2022-33995

3、SAP 产品安全漏洞

SAP 3D Visual Enterprise Viewer 是德国思爱普（SAP）公司的一款 3D 视图查看器。该软件支持在所有行业标准的桌面应用中发布 2D、3D 场景，并支持以独立可执行程序和 ActiveX 空间单独安装。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应用程序崩溃等。

CNVD 收录的相关漏洞包括：SAP 3D Visual Enterprise Viewer 输入验证错误漏洞（CNVD-2022-33129、CNVD-2022-33128、CNVD-2022-33127、CNVD-2022-33126、CNVD-2022-33132、CNVD-2022-33131、CNVD-2022-33130）、SAP 3D Visual Enterprise Viewer 越界写入漏洞。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-2022-33129

https://www.cnvd.org.cn/flaw/show/CNVD-2022-33128

https://www.cnvd.org.cn/flaw/show/CNVD-2022-33127

https://www.cnvd.org.cn/flaw/show/CNVD-2022-33126

https://www.cnvd.org.cn/flaw/show/CNVD-2022-33132

https://www.cnvd.org.cn/flaw/show/CNVD-2022-33131

https://www.cnvd.org.cn/flaw/show/CNVD-2022-33130

https://www.cnvd.org.cn/flaw/show/CNVD-2022-33135

4、Dell 产品安全漏洞

Dell PowerScale OneFS 是提供横向扩展 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敏感信息，在系统上获得提升的权限，导致拒绝服务等。

CNVD 收录的相关漏洞包括：Dell PowerScale OneFS 安全绕过漏洞（CNVD-2022-32806、CNVD-2022-32807）、Dell PowerScale OneFS 拒绝服务漏洞（CNVD-2022-32805、CNVD-2022-32824、CNVD-2022-32826）、Dell PowerScale OneFS 信息泄露漏洞（CNVD-2022-32834、CNVD-2022-32833）、Dell PowerScale OneFS 权限提升漏洞（CNVD-2022-32838）。其中，“Dell PowerScale OneFS 安全绕过漏洞（CNVD-2022-32806、CNVD-2022-32807）、Dell PowerScale OneFS 权限提升漏洞（CNVD-2022-32838）”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-2022-32806

https://www.cnvd.org.cn/flaw/show/CNVD-2022-32807

https://www.cnvd.org.cn/flaw/show/CNVD-2022-32805

https://www.cnvd.org.cn/flaw/show/CNVD-2022-32824

https://www.cnvd.org.cn/flaw/show/CNVD-2022-32826

https://www.cnvd.org.cn/flaw/show/CNVD-2022-32834

https://www.cnvd.org.cn/flaw/show/CNVD-2022-32833

https://www.cnvd.org.cn/flaw/show/CNVD-2022-32838

5、IBM QRadar SIEM 信息泄露漏洞（CNVD-2022-34982）

IBM QRadar SIEM 是美国 IBM 公司的一套利用安全智能保护资产和信息远离高级威胁的解决方案。该方案提供对整个 IT 架构范围进行监督、生成详细的数据访问和用户活动报告等功能。本周，IBM QRadar SIEM 被披露存在信息泄露漏洞。攻击者可利用该漏洞获取日志文件。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-2022-34982

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-2022-32821	Xiaomi MIUI 权限提升漏洞	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://trust.mi.com/zh-CN/misrc/bulletins/advisory?cveId=134
CNVD-2022-32820	ASUS WebStorage Android 安全绕过漏洞	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.asuswebstorage.com/navigate/a/#/index
CNVD-2022-33807	Chamilo LMS SQL 注入漏洞（CNVD-2022-33807）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://support.chamilo.org/projects/1/wiki/Security_issues
CNVD-2022-33820	Myucms 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://www.myucms.com/lists.html
CNVD-2022-33823	Elite Graphix Elite Cms 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://github.com/jsjbcyber/bug_report/blob/main/bug_a

CNVD-2022-34639	Apex Central 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://success.trendmicro.com/solution/000290678
CNVD-2022-35423	Accusoft ImageGear 堆缓冲区溢出漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.accusoft.com/products/imagegear-collection/
CNVD-2022-35519	F5 BIG-IP iControl REST 身份认证绕过漏洞	高	用户可参考如下供应商提供的安全公告获得补丁信息：https://support.f5.com/csp/article/K55879220
CNVD-2022-32819	ASUS RT-AX88U 代码执行漏洞	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.asus.com/Networking-IoT-Servers/WiFi-Routers/ASUS-Gaming-Routers/RT-AX88U/
CNVD-2022-33825	Elite Graphix Elite Cms 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://github.com/jsjbcyber/bug_report/blob/main/bug_c

小结：本周，Google 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，任意修改和设置系统属性，升级权限等。此外，Oracle、SAP、Dell 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，在系统上获得提升的权限，导致应用程序崩溃等。另外，IBM QRadar SIEM 披露存在信息泄露漏洞，攻击者可利用该漏洞获取日志文件。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、Tenda M3 命令注入漏洞（CNVD-2022-33113）

验证描述

Tenda M3 是中国腾达（Tenda）公司的一款门禁控制器。

Tenda M3 存在命令注入漏洞，该漏洞源于组件/goform/WriteFacMac 未能正确过滤构造命令特殊字符、命令等，攻击者可利用该漏洞导致任意命令执行。

验证信息

POC 链接：https://github.com/GD008/vuln/blob/main/tenda_M3_WriteFacMac/M3_WriteFacMac.md

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2022-33113

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. Linux Nimbuspwn 漏洞可能允许攻击者部署复杂的威胁

近期，Microsoft 365 Defender 研究团队发现了两个名为“Nimbuspwn”的 Linux 提权漏洞（编号为 CVE-2022-29799 和 CVE-2022-29800），攻击者可以利用该漏洞进行各种恶意活动，包括部署恶意软件。根据微软发布的公告，这些漏洞可以链接在一起以获得 Linux 系统的 root 权限，允许攻击者部署有效负载，如 root 后门，并通过执行任意 root 代码从而达到运行其他恶意操作的目的。通过利用这些漏洞来实现对目标系统 root 的访问权，并部署更复杂的威胁，例如勒索软件。

参考链接：https://www.freebuf.com/news/331572.html

2. 微软修复了暴露用户数据库的 ExtraReplica Azure 漏洞

近期，微软表示已修复 Azure Database for PostgreSQL Flexible Server 中发现的一系列安全漏洞，这些漏洞可能让恶意用户在绕过身份验证后提升权限并获得对其他客户数据库的访问权限。Flexible Server 部署选项使客户能够最大程度地控制其数据库，包括精细调整和多个配置参数。

参考链接：https://www.freebuf.com/news/331712.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