国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2023 年 03 月 20 日-2023 年 03 月 26 日　　2023 年第 12 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 381 个，其中高危漏洞 161 个、中危漏洞 180 个、低危漏洞 40 个。漏洞平均分值为 6.34。本周收录的漏洞中，涉及 0day 漏洞 331 个（占 87%），其中互联网上出现“Tenda AC18 堆栈溢出漏洞、Eolinker goku_lite 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漏洞总数 16489 个，与上周（30996 个）环比减少 47%。

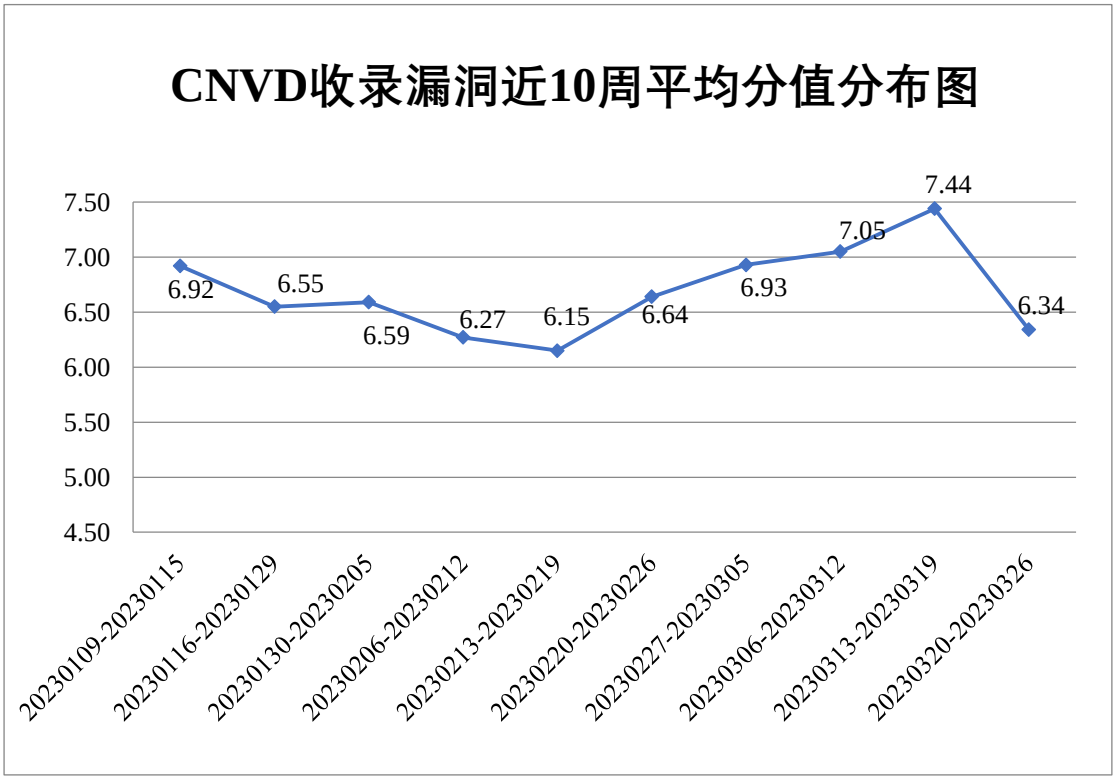

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 17 起，向基础电信企业通报漏洞事件 100 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 1210 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 174 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 81 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、珠海派诺科技股份有限公司、重庆中联信息产业有限责任公司、重庆远秋科技股份有限公司、中企动力科技股份有限公司、中科可控信息产业有限公司、智互联（深圳）科技有限公司、正泰安能数字能源（浙江）股份有限公司、浙江浙大中控信息技术有限公司、浙江宇视科技有限公司、浙江永拓信息科技有限公司、掌如科技服务有限公司、长春云谷科技有限公司、漳州豆壳网络科技有限公司、友讯电子设备（上海）有限公司、用友网络科技股份有限公司、烟台海能仪表科技有限公司、信呼、新天科技股份有限公司、新开普电子股份有限公司、西门子（中国）有限公司、西安众邦网络科技有限公司、西安点测网络科技有限公司、武汉易维科技股份有限公司、望海康信（北京）科技股份公司、天津众齐软件股份有限公司、天地伟业技术有限公司、天地（常州）自动化股份有限公司、台达电子企业管理(上海)有限公司、苏州科达科技股份有限公司、苏州汇川技术有限公司、四川鱼尾巴科技有限公司、四川思途智旅软件有限公司、深圳友联科技有限公司、深圳维盟科技股份有限公司、深圳拓安信物联股份有限公司、深圳市网心科技有限公司、深圳市拓普泰尔科技有限公司、深圳市赛蓝科技有限公司、深圳市金蝶天燕云计算股份有限公司、深圳市捷道智控实业有限公司、深圳市吉祥腾达科技有限公司、深圳市河辰通讯技术有限公司、深圳市合信自动化技术有限公司、深圳市海融易通电子有限公司、深圳市触拓科技有限公司、深圳科士达科技股份有限公司、上海卓卓网络科技有限公司、上海商派网络科技有限公司、上海梦创双杨数据科技股份有限公司、上海居亦科技发展有限公司、上海费浦安防技术有限公司、上海泛微网络科技股份有限公司、上海阿法迪智能数字科技股份有限公司、商丘芝麻开门网络科技有限公司、山东金田水利科技有限公司、山东德尔智能数码股份有限公司、山东比特智能科技股份有限公司、厦门宇电自动化科技有限公司、厦门一指通智能科技有限公司、厦门网中网软件有限公司、厦门四信通信科技有限公司、厦门纳龙健康科技股份有限公司、青岛东软载波科技股份有限公司、普联技术有限公司、鹏为软件股份有限公司、明腾网络股份有限公司、美团安全应急响应中心、矩阵起源（深圳）信息科技有限公司、江苏曼荼罗软件股份有限公司、吉翁电子（深圳）有限公司、湖南强智科技发展有限公司、湖南建研信息技术股份有限公司、湖南奥科网络技术股份有限公司、湖北京山轻工机械股份有限公司、红门智能科技股份有限公司、弘扬软件股份有限公司、河北

品科信息科技有限公司、杭州智诺科技股份有限公司、杭州云朵科技有限公司、杭州映云科技有限公司、杭州萤石网络股份有限公司、杭州雄伟科技开发股份有限公司、杭州新中大科技股份有限公司、杭州三汇信息工程有限公司、杭州海康威视系统技术有限公司、杭州博采网络科技股份有限公司、广州红帆科技有限公司、广州超远机电科技有限公司、广联达科技股份有限公司、广东优信无限网络股份有限公司、广东弘智科技有限公司、福建瑞术信息科技有限公司、迪讯信息技术有限公司、大连理工计算机控制工程有限公司、成都星锐蓝海网络科技有限公司、成都四相致新科技有限公司、成都生动网络科技有限公司、畅捷通信息技术股份有限公司、北京卓众出版有限公司、北京中新天达科技有限公司、北京中成科信科技发展有限公司、北京优炫软件股份有限公司、北京亚控科技发展有限公司、北京星网锐捷网络技术有限公司、北京夕阳无忧科技有限公司、北京通达信科科技有限公司、北京数字政通科技股份有限公司、北京神州数码云科信息技术有限公司、北京美特软件技术有限公司、北京猎鹰安全科技有限公司、北京久其软件股份有限公司、北京金和网络股份有限公司、北京杰控科技有限公司、北京火绒网络科技有限公司、北京宏景世纪软件股份有限公司、北京百卓网络技术有限公司、北京奥博威斯科技有限公司、安徽银通物联有限公司、Oki Electric Industry Co., Ltd 和 Axis Communications AB。

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、安天科技集团股份有限公司、北京启明星辰信息安全技术有限公司、阿里云计算有限公司等单位报送公开收集的漏洞数量较多。北京华顺信安信息技术有限公司、北京升鑫网络科技有限公司、快页信息技术有限公司、上海齐同信息科技有限公司、河南东方云盾信息技术有限公司、山东鼎夏智能科技有限公司、北京山石网科信息技术有限公司、浙江安腾信息技术有限公司、杭州美创科技有限公司、博智安全科技股份有限公司、杭州默安科技有限公司、重庆都会信息科技有限公司、湖南轻山信息技术有限公司、河南信安世纪科技有限公司、安徽锋刃信息科技有限公司、北京大学、汇安云（山东）信息科技有限公司、江西诚韬科技有限公司、北京赛博昆仑科技有限公司、河南灵创电子科技有限公司、北京华云安信息技术有限公司、海南神州希望网络有限公司、北京珞安科技有限责任公司、赛尔网络有限公司、江苏金盾检测技术有限公司、平安银河实验室、北京远禾科技有限公司、福建奇比特信息科技有限公司、华泰证券股份有限公司、宁夏凯信特信息科技有限公司、北京威努特技术有限公司、上海银行股份有限公司、上海纽盾科技股份有限公司、河北千诚电子科技有限公司、苏州棱镜七彩信息科技有限公司、郑州埃文科技、华堡天建（天津）信息技术有限公司、北京六方云信息技术有限公司、北京微步在线科技有限公司、北京原创先锋网络科技发展有限公司、北京惠而特科技有限

公司、广东唯顶信息科技股份有限公司、奇安星城网络安全运营服务（长沙）有限公司、上海天存信息技术有限公司、京数安（北京）科技有限公司、北方实验室（沈阳）股份有限公司、任子行网络技术股份有限公司及其他个人白帽子向 CNVD 提交了 16489 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）、三六零数字安全科技集团有限公司和上海交大向CNVD共享的白帽子报送的13396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）	8172	8172
奇安信网神（补天平台）	3313	3313
三六零数字安全科技集团有限公司	1112	1112
上海交大	799	799
深信服科技股份有限公司	518	0
新华三技术有限公司	404	0
安天科技集团股份有限公司	292	0
北京启明星辰信息安全技术有限公司	242	8
阿里云计算有限公司	175	14
杭州安恒信息技术股份有限公司	116	116
沈阳东软系统集成工程有限公司	45	0
恒安嘉新（北京）科技股份公司	37	0
中国电信集团系统集成有限责任公司	30	0
京东科技信息技术有限公司	20	0
远江盛邦（北京）网络安全科技股份有限公司	19	19

杭州迪普科技股份有限公司	14	0
北京天融信网络安全技术有限公司	9	9
南京众智维信息科技有限公司	4	4
北京知道创宇信息技术股份有限公司	3	0
西安四叶草信息技术有限公司	3	3
北京信联数安科技有限公司	1	1
北京智游网安科技有限公司	1	1
北京华顺信安信息技术有限公司	357	1
北京升鑫网络科技有限公司	241	241
快页信息技术有限公司	133	133
上海齐同信息科技有限公司	68	68
河南东方云盾信息技术有限公司	41	41
山东鼎夏智能科技有限公司	40	40
北京山石网科信息技术有限公司	36	36
浙江安腾信息技术有限公司	26	26
杭州美创科技有限公司	23	23
博智安全科技股份有限公司	23	23
杭州默安科技有限公	21	21

司		
重庆都会信息科技有限公司	15	15
湖南轻山信息技术有限公司	15	15
河南信安世纪科技有限公司	14	14
安徽锋刃信息科技有限公司	10	10
北京大学	10	10
汇安云（山东）信息科技有限公司	9	9
江西诚韬科技有限公司	8	8
北京赛博昆仑科技有限公司	8	8
任子行网络技术股份有限公司	7	7
河南灵创电子科技有限公司	5	5
北京华云安信息技术有限公司	5	5
海南神州希望网络有限公司	3	3
北京珞安科技有限责任公司	3	3
赛尔网络有限公司	3	3
江苏金盾检测技术有限公司	3	3
平安银河实验室	2	2
北京远禾科技有限公司	2	2
福建奇比特信息科技有限公司	2	2
华泰证券股份有限公	2	2

司		
宁夏凯信特信息科技有限公司	2	2
北京威努特技术有限公司	2	2
上海银行股份有限公司	2	2
上海纽盾科技股份有限公司	2	2
亚信科技（成都）有限公司	2	0
河北千诚电子科技有限公司	1	1
苏州棱镜七彩信息科技有限公司	1	1
郑州埃文科技	1	1
华堡天建（天津）信息技术有限公司	1	1
北京六方云信息技术有限公司	1	1
北京微步在线科技有限公司	1	1
北京原创先锋网络科技发展有限公司	1	1
北京惠而特科技有限公司	1	1
广东唯顶信息科技股份有限公司	1	1
奇安星城网络安全运营服务（长沙）有限公司	1	1
上海天存信息技术有限公司	1	1
京数安（北京）科技有限公司	1	1

北方实验室（沈阳）股份有限公司	1	1
CNCERT 广西分中心	13	13
CNCERT 贵州分中心	3	3
CNCERT 北京分中心	1	1
个人	2101	2101
报送总计	18605	16489

本周漏洞按类型和厂商统计

本周，CNVD 收录了 381 个漏洞。WEB 应用 165 个，应用程序 86 个，网络设备（交换机、路由器等网络端设备）83 个，智能设备 21 个，操作系统 14 个，安全产品 11 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	165
应用程序	86
网络设备（交换机、路由器等网络端设备）	83
智能设备	21
操作系统	14
安全产品	11
数据库	1

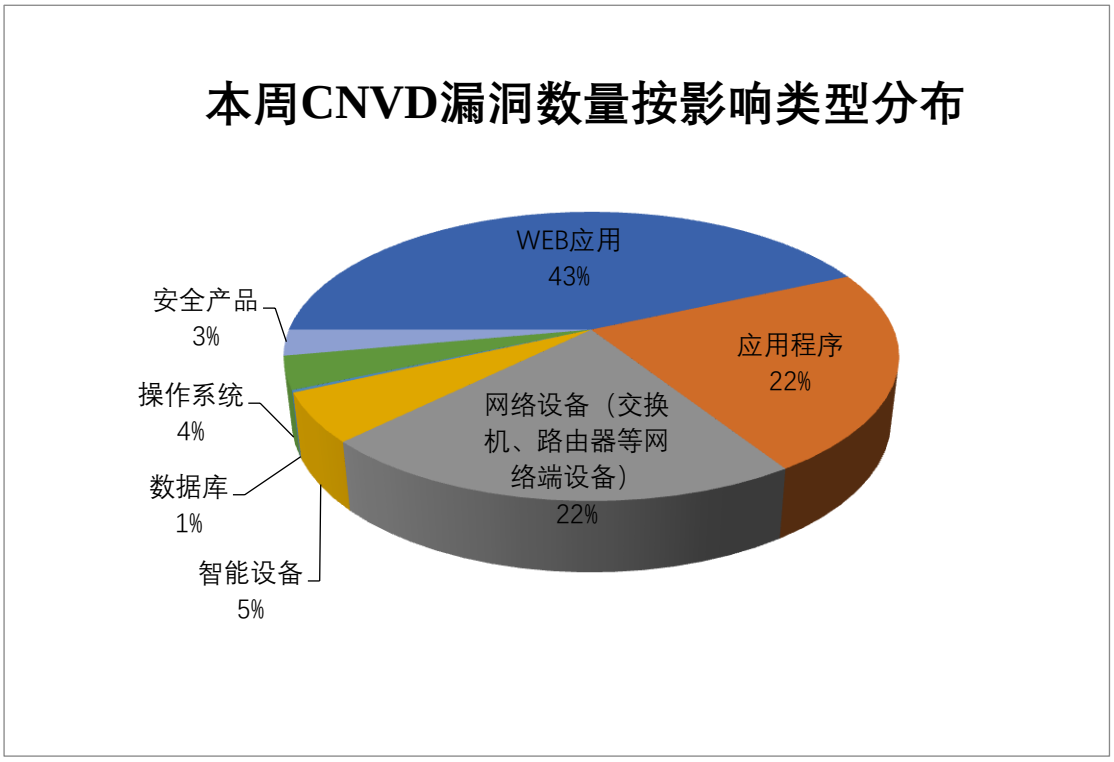

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 TRENDnet、Tenda、Fortinet 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	TRENDnet	20	5%
2	Tenda	16	5%
3	Fortinet	11	3%
4	Google	10	3%
5	TOTOLINK	9	2%
6	SIEMENS	9	2%
7	Microsoft	8	2%
8	MayiCMS	7	2%
9	Hippo4J	4	1%
10	其他	287	75%

本周行业漏洞收录情况

本周，CNVD 收录了 68 个电信行业漏洞，57 个移动互联网行业漏洞，10 个工控行业漏洞（如下图所示）。其中，“Siemens Tecnomatix Plant Simulation 堆栈缓冲区溢出漏洞、Tenda W6-S 命令注入漏洞、Google Android 权限提升漏洞（CNVD-2023-18914）”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 C

NVD 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/

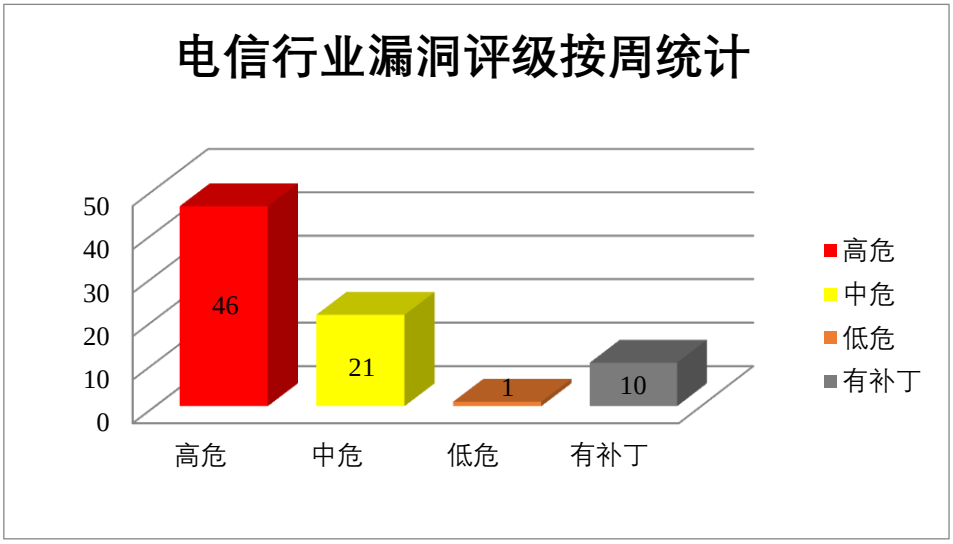

图 3 电信行业漏洞统计

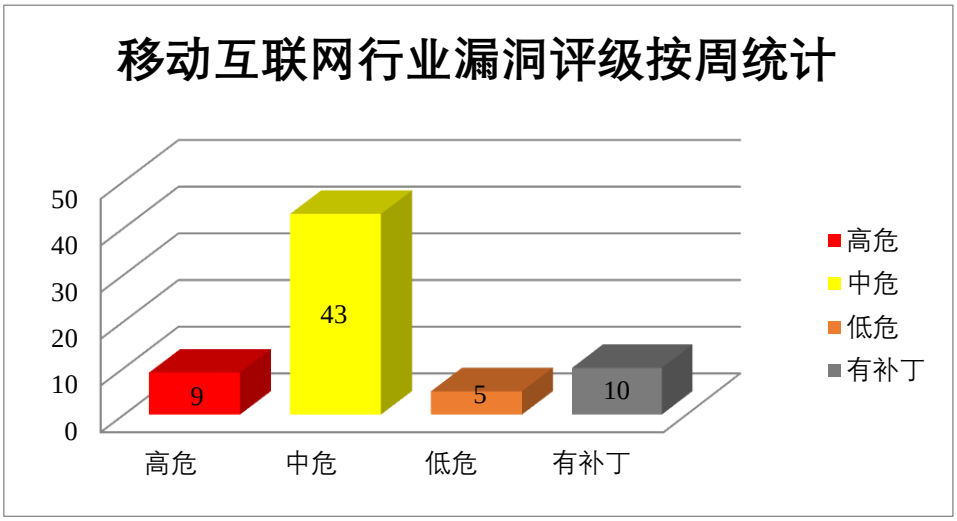

图 4 移动互联网行业漏洞统计

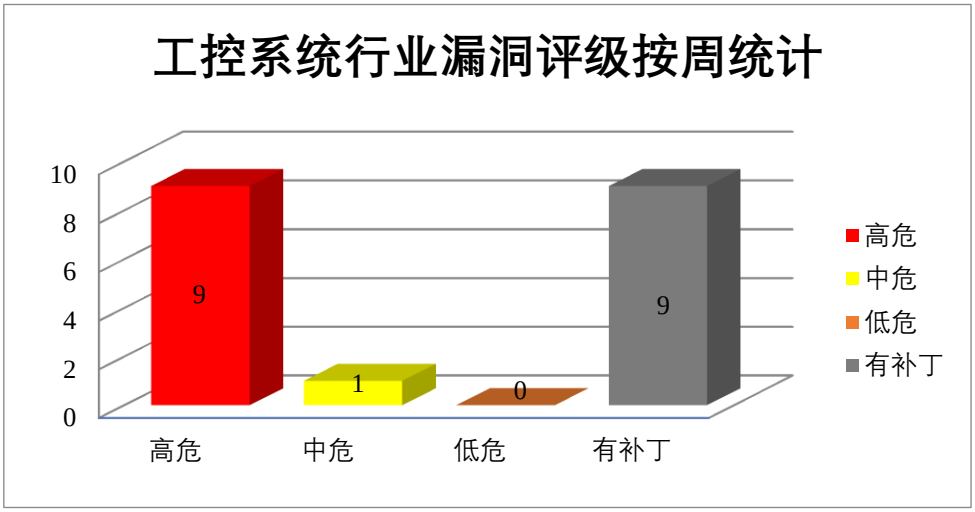

图 5 工控系统行业漏洞统计

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，提升权限，造成拒绝服务。

CNVD 收录的相关漏洞包括：Google Android 信息泄露漏洞（CNVD-2023-18906）、Google Android 拒绝服务漏洞（CNVD-2023-18908、CNVD-2023-18909）、Google Android 权限提升漏洞（CNVD-2023-18910、CNVD-2023-18915、CNVD-2023-18912、CNVD-2023-18913、CNVD-2023-18914）。其中，除“Google Android 信息泄露漏洞（CNVD-2023-18906）、Google Android 拒绝服务漏洞（CNVD-2023-18908、CNVD-2023-18909）”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-2023-18906

https://www.cnvd.org.cn/flaw/show/CNVD-2023-18908

https://www.cnvd.org.cn/flaw/show/CNVD-2023-18909

https://www.cnvd.org.cn/flaw/show/CNVD-2023-18910

https://www.cnvd.org.cn/flaw/show/CNVD-2023-18915

https://www.cnvd.org.cn/flaw/show/CNVD-2023-18912

https://www.cnvd.org.cn/flaw/show/CNVD-2023-18913

https://www.cnvd.org.cn/flaw/show/CNVD-2023-18914

2、 Microsoft 产品安全漏洞

Microsoft Windows Bluetooth Service 是美国微软（Microsoft）公司的一个蓝牙驱动程序。Microsoft Office 是微软公司开发的一套基于 Windows 操作系统的办公软件套装。Microsoft Windows 是一款由美国微软公司开发的窗口化操作系统。Microsoft Exchange Server 是美国微软（Microsoft）公司的一套电子邮件服务程序。它提供邮件存取、储存、转发，语音邮件，邮件过滤筛选等功能。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，在目标主机上执行代码。

CNVD 收录的相关漏洞包括：Microsoft Windows Bluetooth Service 代码执行漏洞、Microsoft Exchange Server 远程代码执行漏洞（CNVD-2023-18284）、Microsoft Office 信息泄露漏洞（CNVD-2023-18285）、Microsoft Windows Malicious Software Removal Tool 权限提升漏洞、Microsoft Office 远程代码执行漏洞（CNVD-2023-18287、CNVD-2023-18288）、Microsoft Office Visio 远程代码执行漏洞（CNVD-2023-18289）、Microsoft Windows Kernel 权限提升漏洞（CNVD-2023-18290）。其中，除“Microsoft Office 信息泄露漏洞（CNVD-2023-18285）、Microsoft Windows Malicious Software Removal Tool 权限提升漏洞”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-2023-18283
https://www.cnvd.org.cn/flaw/show/CNVD-2023-18284
https://www.cnvd.org.cn/flaw/show/CNVD-2023-18285
https://www.cnvd.org.cn/flaw/show/CNVD-2023-18286
https://www.cnvd.org.cn/flaw/show/CNVD-2023-18287
https://www.cnvd.org.cn/flaw/show/CNVD-2023-18288
https://www.cnvd.org.cn/flaw/show/CNVD-2023-18289
https://www.cnvd.org.cn/flaw/show/CNVD-2023-18290

3、Fortinet 产品安全漏洞

Fortinet FortiWeb 是美国飞塔（Fortinet）公司的一款 Web 应用层防火墙，它能够阻断如跨站点脚本、SQL 注入、Cookie 中毒、schema 中毒等攻击的威胁。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特制的 HTTP GET 请求获取对文件和数据的未经授权访问，提升权限，执行任意代码或命令等。

CNVD 收录的相关漏洞包括：Fortinet FortiWeb 操作系统命令注入漏洞（CNVD-2023-18291）、Fortinet FortiWeb 格式化字符串错误漏洞、Fortinet FortiWeb 缓冲区溢出漏洞（CNVD-2023-18294、CNVD-2023-18297、CNVD-2023-18301、CNVD-2023-18300）、Fortinet FortiWeb 路径遍历漏洞（CNVD-2023-18293）、Fortinet FortiWeb 资源管理错误漏洞。其中，“Fortinet FortiWeb 操作系统命令注入漏洞（CNVD-2023-18291）、Fortinet FortiWeb 缓冲区溢出漏洞（CNVD-2023-18294、CNVD-2023-18297、CNVD-2023

-18300）”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-2023-18291
https://www.cnvd.org.cn/flaw/show/CNVD-2023-18295
https://www.cnvd.org.cn/flaw/show/CNVD-2023-18294
https://www.cnvd.org.cn/flaw/show/CNVD-2023-18293
https://www.cnvd.org.cn/flaw/show/CNVD-2023-18298
https://www.cnvd.org.cn/flaw/show/CNVD-2023-18297
https://www.cnvd.org.cn/flaw/show/CNVD-2023-18301
https://www.cnvd.org.cn/flaw/show/CNVD-2023-18300

4、Siemens 产品安全漏洞

Siemens Tecnomatix Plant Simulation 是德国西门子（Siemens）公司的一个工控设备。利用离散事件仿真的功能进行生产量分析和优化，进而改善制造系统性能。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进程的上下文中执行代码。

CNVD 收录的相关漏洞包括：Siemens Tecnomatix Plant Simulation 堆栈缓冲区溢出漏洞（CNVD-2023-18928、CNVD-2023-18933）、Siemens Tecnomatix Plant Simulation 越界读取漏洞（CNVD-2023-18929、CNVD-2023-18932、CNVD-2023-18935）、Siemens Tecnomatix Plant Simulation 越界写入漏洞（CNVD-2023-18930、CNVD-2023-18931）、Siemens Tecnomatix Plant Simulation 内存破坏漏洞。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-2023-18928
https://www.cnvd.org.cn/flaw/show/CNVD-2023-18929
https://www.cnvd.org.cn/flaw/show/CNVD-2023-18930
https://www.cnvd.org.cn/flaw/show/CNVD-2023-18931
https://www.cnvd.org.cn/flaw/show/CNVD-2023-18932
https://www.cnvd.org.cn/flaw/show/CNVD-2023-18933
https://www.cnvd.org.cn/flaw/show/CNVD-2023-18934
https://www.cnvd.org.cn/flaw/show/CNVD-2023-18935

5、TRENDnet TEW-755AP 缓冲区溢出漏洞

TRENDnet TEW-755AP 是美国趋势网络（TRENDnet）公司的一款路由器。本周，TRENDnet TEW-755AP 被披露存在缓冲区溢出漏洞。该漏洞源于 wifi_captive_portal 函数中的 user_edit_page 参数对输入的数据缺乏大小检查，攻击者可利用该漏洞在系统上执行任意代码。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-20

23-18937

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：https://www.cnvd.org.cn/flaw/list

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-2023-18926	Tenda W6-S 拒绝服务漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：https://www.tenda.com.cn/default.html
CNVD-2023-18289	Microsoft Office Visio 远程代码执行漏洞（CNVD-2023-18289）	高	目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载：https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-21736
CNVD-2023-18914	Google Android 权限提升漏洞（CNVD-2023-18914）	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：https://source.android.com/docs/security/bulletin/2023-01-01
CNVD-2023-18918	Tenda W30E 堆栈溢出漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：https://www.tenda.com.cn/default.html
CNVD-2023-18936	Siemens Tecnomatix Plant Simulation 越界写入漏洞（CNVD-2023-18936）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://cert-portal.siemens.com/productcert/pdf/ssa-847261.pdf
CNVD-2023-19774	Parallels Desktop for Mac 产品中 Toolgate 组件路径穿越漏洞	高	用户可联系供应商获得补丁信息：https://www.parallels.cn/products/desktop/
CNVD-2023-19953	MinIO 信息泄露漏洞	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/minio/minio/security/advisories/GHSA-6xvq-wj2x-3h3q
CNVD-2023-18288	Microsoft Office 远程代码执行漏洞（CNVD-2023-18288）	高	目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载：https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2023-21735
CNVD-2023-18913	Google Android 权限提升漏洞（CNVD-2023-18913）	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：

			https://source.android.com/docs/security/bulletin/2023-01-01
CNVD-2023-18925	Tenda W6-S 命令注入漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：https://www.tenda.com.cn/default.html

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，提升权限，造成拒绝服务。此外，Microsoft、Fortinet、Siemens 等多款产品被披露存在多个漏洞，攻击者可利用漏洞通过特制的 HTTP GET 请求获取对文件和数据的未经授权访问，提升权限，执行任意代码或命令等。另外，TRENDnet TEW-755AP 被披露存在缓冲区溢出漏洞。攻击者可利用该漏洞在系统上执行任意代码。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、Tenda AC18 堆栈溢出漏洞

验证描述

Tenda AC18 是中国腾达（Tenda）公司的一款路由器。

Tenda AC18 存在堆栈溢出漏洞，该漏洞源于 fromSetSysTime 函数的 time 参数对于输入数据缺乏长度验证。攻击者可利用漏洞导致拒绝服务。

验证信息

POC 链接：https://drive.google.com/file/d/1elSFijqHselDzRNuawGfcHD4uL4N8_mM/view

参考链接：https://www.cnvd.org.cn/flaw/show/CNVD-2023-18958

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. CISA 警告潜伏在关键基础设施中的未修补 ICS 漏洞

美国网络安全和基础设施安全局（CISA）本周发布了针对多个关键基础设施部门中使用的八个工业控制系统（ICS）中的 49 个漏洞的公告，其中一些尚未修补。

参考链接：https://www.darkreading.com/vulnerabilities-threats/cisa-warns-unpatched-vulnerabilities-ics-critical-infrastructure

2. 微软 Win10/Win11 系统同样存在 Pixel 手机漏洞：可部分还原已修剪图片

微软 Win11 系统原生的 Windows Snipping Tool、Win10 系统中原生的“Snip & Sketch”截图同样存在 aCropalypse 漏洞，通过将图像格式从 RGB 修改为 RGBA，同样可以还原修剪操作之后的原图信息。

参考链接：https://www.ithome.com/0/681/412.htm

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