ICS 35.240.50
CCS L 62

团　　体　　标　　准

T/CPUMT 008—2022

工业信息安全漏洞分类分级指南

Guidelines for categorization and classification of industrial information security vulnerability

2022-11-08 发布　　2022-11-08 实施

中国和平利用军工技术协会　发布
中国标准出版社　出版

目　　次

前　言

本文件按照 GB/T 1.1—2020《标准化工作导则　第 1 部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中国和平利用军工技术协会提出并归口。

本文件起草单位：国家工业信息安全发展研究中心、浙江木链物联网科技有限公司、联通数字科技有限公司、北京天融信网络安全技术有限公司、成都安美勤信息技术股份有限公司、浙江中控技术股份有限公司、奇安信科技集团股份有限公司、北京国泰网信科技有限公司、飞诺门阵（北京）科技有限公司、新华三技术有限公司、北京六方云信息技术有限公司、浪潮工业互联网股份有限公司、北京珞安科技有限责任公司、上海市网络技术综合应用研究所、杭州中电安科现代科技有限公司、深圳市盛视技术有限公司、重庆中科摇橹船信息科技有限公司、博智安全科技股份有限公司、深圳市德传技术有限公司、河南金盾信安检测评估中心有限公司、北京声智科技有限公司、宁波和利时信息安全研究院有限公司、成都久信信息技术股份有限公司、北京控制与电子技术研究所、苏州国芯科技股份有限公司、亚信安全科技股份有限公司、新疆量子通信技术有限公司、西北工业大学、北京邮电大学、上汽通用五菱汽车股份有限公司、北京北武安信科技有限公司、中国移动通信集团福建有限公司泉州分公司、中国兵器装备集团有限公司、中国电子信息产业集团有限公司第六研究所、中国电子科技集团公司第十五研究所、公安部第一研究所、公安部第三研究所、国家信息技术安全研究中心、北京中科北斗技术研究院、上海大学、空间视创（重庆）科技股份有限公司、北京通明湖信息技术应用创新中心、国网新疆电力有限公司电力科学研究院、北京关键科技股份有限公司、参数技术（上海）软件有限公司、同方工业信息技术有限公司、上海计算机软件技术开发中心、首钢京唐钢铁联合有限责任公司、浙江安远检测技术有限公司、河南天祺信息安全技术有限公司、北京蓝象标准咨询服务有限公司。

本文件主要起草人：杨安、郭宾、孙涛、袁留记、李劲雄、丰存旭、王戬、李欣、沈寓实、李刚、周永权、商广勇、肖智中、徐绍飞、张俊峰、曹美玲、郑道勤、傅涛、黄齐雄、梁宏、陈孝良、乐翔、朱光剑、李晓龙、匡启和、楚鹏、邓璐、杨黎斌、崔宝江、俸文都、郝晓夜、吴有祥、安维嵘、王绍杰、刘健、陈彦如、田原、方进社、崔慧霞、袁建军、刘才果、曹军威、杨慧婷、张怀珠、郎燕、汪志水、李爽、周华中、徐晓翔、刘向东、张孟、雷濛、张婧宇、余梦达、易拓、张子钰、徐伟、龚沫薇、王世轶、姚蒙蒙、张俊林、曹锋、段小莉、张德保、马建红、乔华阳。

引　言

工业信息安全漏洞是在整个工业运转过程中，存在于工业领域专有的、非通用信息技术的软件、硬件、协议、系统中，对工业信息、工业领域各个环节甚至经济进展与社会稳定造成影响的漏洞，这些漏洞对工业控制系统的安全（机密性、完整性、可用性）和生产过程稳定性产生重要影响。工业信息安全漏洞分类分级包含工业信息安全漏洞分类、工业信息安全漏洞分级指标、工业信息安全漏洞危害分级等内容，明确了工业信息安全漏洞所属类型，研判工业信息安全漏洞触发对工业领域产品、协议及相关使用环境造成的危害程度。

制定本文件旨在提供工业信息安全漏洞的分类方法、分级方法等信息，首先可协助工业信息安全人员准确识别未知漏洞的类型和危害程度，有针对性地选择分析手法和技术；其次可指导工业信息安全漏洞相关产品的研发、使用，提高工业信息安全人员的漏洞分析和应急处置能力，协助工业领域产品提供者及时确定漏洞修复方案，辅助工业信息安全应急处置人员及时采用准确的处置方案，降低漏洞对工业领域产品、协议或工业现场的影响；此外，加快制定工业信息安全漏洞分类分级相关标准，建设完善工业信息安全漏洞标准体系，有利于推动我国工业信息安全漏洞管理工作自动化、高效化发展。

工业信息安全漏洞分类分级指南

1 范围

本文件提供了工业信息安全漏洞的分类方法、分级指标和危害分级等建议。

本文件适用于工业领域的软硬件产品提供者、工业信息安全漏洞收集组织、工业信息安全漏洞应急组织在漏洞管理、技术研发等活动中的漏洞分类和分级评估。工业领域产品提供者、工业领域产品运营者的漏洞分类分级可参照使用。

2 规范性引用文件

本文件没有规范性引用文件。

3 术语和定义

下列术语和定义适用于本文件。

3.1

工业信息安全漏洞 industrial information security vulnerability

在整个工业运转过程中，存在于工业领域专有的、非通用信息技术的软件、硬件、协议、系统中，对工业信息、工业领域各个环节甚至经济进展与社会稳定造成影响的漏洞。

3.2

受影响实体 impacted entity

工业信息安全漏洞触发时，其直接影响的工业领域专有硬件、协议、软件、系统等具体实体对象。

示例：可编程控制器、工业控制协议、工业控制软件等。

4 缩略语

下列缩略语适用于本文件。

APP：移动智能终端应用软件(Application)

DCS：集散控制系统(Distributed Control System)

DTU：数据传输单元(Data Transfer Unit)

I/O：输入/输出(Input/Output)

OLE：对象连接与嵌入(Object Linking and Embedding)

OPC：对象链接与嵌入的过程控制(OLE for Process Control)

PLC：可编程控制器(Programmable Logic Controller)

RTU：远程终端单元(Remote Terminal Unit)

SQL：结构化查询语言(Structured Query Language)

WEB：全球广域网或万维网(World Wide Web)