ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 44886.4—2026
代替 GB/T 36643—2018

网络安全技术　网络安全产品互联互通 第4部分：威胁信息格式

Cybersecurity technology—Cybersecurity product interconnectivity—Part 4：Threat information format

2026-07-02 发布　　2027-02-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前言 …… Ⅲ
引言 …… Ⅳ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 1
4　缩略语 …… 2
5　概述 …… 2
6　组件的结构及公共属性 …… 5
7　组件 …… 7
8　关系组件 …… 24
附录 A（规范性）　字段类型描述 …… 26
附录 B（规范性）　模式语言的描述 …… 28
附录 C（规范性）　可观测数据子组件 …… 37
附录 D（规范性）　词汇表 …… 52
附录 E（资料性）　威胁信息封装和解析方式 …… 68
附录 F（资料性）　威胁信息组件示例的 JSON 表示 …… 69
附录 G（资料性）　组件关系汇总 …… 78
附录 H（资料性）　部分攻击场景下威胁信息描述示例 …… 80
附录 I（资料性）　表达式计算示例 …… 92
参考文献 …… 94

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。

本文件是GB/T 44886《网络安全技术　网络安全产品互联互通》的第4部分。GB/T 44886已经发布了以下部分：

——第1部分：框架；

——第2部分：资产信息格式；

——第3部分：告警信息格式；

——第4部分：威胁信息格式；

——第5部分：行为信息格式。

本文件代替GB/T 36643—2018《信息安全技术　网络安全威胁信息格式规范》，与GB/T 36643—2018相比，除结构调整和编辑性改动外，主要技术变化如下：

a) 增加了网络安全威胁信息互联互通典型应用场景（见5.1）；

b) 更改了网络安全威胁信息描述模型（见5.2，GB/T 36643—2018的第5章）；

c) 增加了“组件结构及公共属性”内容（见第6章）；

d) 删除了“安全事件”组件（见GB/T 36643—2018的6.4）；

e) 更改了“攻击方法”组件描述，将其拆分为“攻击模式”“基础设施”“恶意软件”三个组件进行独立描述（见7.2.1、7.2.2、7.2.5，GB/T 36643—2018的6.6）；

f) 增加了“漏洞”组件实现对攻击目标的描述（见7.2.4）；

g) 更改了可观测数据组件描述和内容（见7.3.1和附录C，GB/T 36643—2018的6.2）；

h) 增加了“工具”“恶意软件分析结果”“攻击活动集”“地理位置”“报告”和“观点”6个组件（见7.2.3、7.2.6、7.3.4、7.4.1、7.4.2、7.4.3）。

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。

本文件由全国网络安全标准化技术委员会（SAC/TC 260）提出并归口。

本文件起草单位：中国电子技术标准化研究院、国家计算机网络应急技术处理协调中心、北京天际友盟信息技术有限公司、北京神州绿盟科技有限公司、华为技术有限公司、天翼安全科技有限公司、中国科学院信息工程研究所、国家信息技术安全研究中心、中国信息安全测评中心、国家信息中心、中国交通通信信息中心、公安部第一研究所、北京航空航天大学、西安电子科技大学、中国科学院计算机网络信息中心、中国人民大学、安徽科技工程大学、杭州安恒信息技术股份有限公司、北京源堡科技有限公司、奇安信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、启明星辰信息技术集团股份有限公司、北京微步在线科技有限公司、长扬科技（北京）股份有限公司、北京长亭科技有限公司、上海斗象信息科技有限公司、远江盛邦安全科技集团股份有限公司、用友网络科技股份有限公司、中广核智能科技（深圳）有限责任公司、中移动信息技术有限公司。

本文件主要起草人：王惠莅、张东举、廖剑、李琳、蔡磊、崔牧凡、翟湛鹏、张宇娜、李强、梁伟、姚叶鹏、秋阳、姚佳明、贺铮、易锦、韩一剑、耿同成、杜渐、伍前红、马文平、习宁、肖彪、秦波、曹浩、涂小毅、梁露露、白敏、晋钢、胡月、张宽、白燕妮、杨大路、赵华、陈联鉴、曾裕智、权晓文、季晟宇、姜政伟、封荣、陈伟雄、冀文、白雪。

本文件及其所代替文件的历次版本发布情况为：

——2018年首次发布为GB/T 36643—2018；

——本次为第一次修订。

引　言

GB/T 44886《网络安全技术　网络安全产品互联互通》是指导网络安全产品互联互通建设的基础性和通用性标准，拟由六个部分构成。

——第1部分：框架。目的在于明确网络安全产品互联互通应用场景，提出互通建设思路。

——第2部分：资产信息格式。目的在于提出网络安全产品互联互通时的资产描述。

——第3部分：告警信息格式。目的在于有效整合网络安全产品报送的告警信息，提高告警应急处置效率。

——第4部分：威胁信息格式。目的在于统一网络安全产品及各组织威胁信息共享格式。

——第5部分：行为信息格式。目的在于促进网络安全产品行为信息的分析利用。

——第6部分：功能接口。目的在于高效整合网络安全信息，促进网络安全产品功能协同。

随着网络攻防对抗博弈的日益加剧，网络攻击方式和攻击手法呈现出多样性、复杂性特点，网络安全威胁具有越来越明显的普遍性和持续性，且攻击者获取攻击工具越来越便利，导致网络攻击成本大大降低，检测网络攻击的难度却越来越大。传统的网络安全防护方案仅仅依靠各个组织独立实施垂直的防护机制，在应对这些复杂网络攻击时显得越来越低效，亟待采取新的技术手段来提升整体网络安全防护能力。

网络安全威胁信息共享和利用是提升整体网络安全防护效率的重要措施，旨在采用多种技术手段，通过采集大规模、多渠道的碎片式攻击或异常数据，集中地进行深度融合、归并和分析，形成与网络安全防护有关的威胁信息线索，并在此基础上进行主动、协同式的网络安全威胁预警、检测和响应，以降低网络安全威胁的防护成本，提升整体的网络安全防护效率。

目前威胁信息来源多样，其描述格式不尽统一。威胁信息是网络安全产品互联互通信息的6类信息之一。规范网络安全威胁信息的格式和交换方式是实现网络安全威胁信息共享和利用的前提和基础。本文件规定了一种结构化方法描述网络安全威胁信息，目的是规范网络安全威胁信息的一致性描述，提升威胁信息的共享效率、互操作性，进而提升整体的网络安全威胁态势感知能力，实现网络安全威胁管理和应用的自动化。

网络安全技术　网络安全产品互联互通 第4部分：威胁信息格式

1　范围

本文件规定了网络安全产品互联互通场景下网络安全威胁信息的格式，包括各组件的属性及组件之间的关系。

本文件适用于网络安全产品生成、使用和威胁信息处理，也为网络安全威胁信息平台的建设和运营提供参考。

2　规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 4754　国民经济行业分类

GB/T 17969.8　信息技术　对象标识符登记机构操作规程　第8部分：通用唯一标识符（UUIDs）的生成及其在对象标识符中的使用

GB/T 25069　信息安全技术　术语

GB/T 28458　信息安全技术　网络安全漏洞标识与描述规范

GB/T 44886.2　网络安全技术　网络安全产品互联互通　第2部分：资产信息格式

IETF RFC 1034　域名　概念和设施（Domain names—Concepts and facilities）

IETF RFC 3986　统一资源标识符（URI）：通用语法［Uniform Resource Identifier（URI）：Generic Syntax］

IETF RFC 5322　互联网消息格式（Internet Message Format）

IETF RFC 5646　语言识别标签（Tags for Identifying Languages）

IETF RFC 5890　面向应用的国际化域名（IDNA）：定义和文档框架［Internationalized Domain Names for Applications（IDNA）：Definitions and Document Framework］

3　术语和定义

GB/T 25069界定的以及下列术语和定义适用于本文件。

3.1

网络安全产品互联互通　cybersecurity product interconnectivity

通过统一的网络安全信息描述和功能接口定义，有效共享网络安全产品感知或产生的信息，协同不同网络安全产品的功能，支撑监测预警、信息共享、应急响应、态势感知等应用，提升网络安全防护能力和网络安全事件处置效率的一种机制。

［来源：GB/T 44886.1—2024，3.2］