为符合欧盟《网络韧性法案》(CRA) 第 14 条做好准备

卷 8 | 期数 32 | 2026 年 6 月
作者： Karl Lau, Tommy Leung; 校对：Joey Kwok

重点摘录

- 欧盟《网络韧性法案》(CRA)，即 (EU) 2024/2847 号条例，对进入欧盟市场的数字产品提出了迄今为止最严格、最全面的网络安全要求。其中，第 14 条——强制性漏洞和事件报告——将于 2026 年 9 月 11 日生效，这意味着制造商只有有限的时间来实施合规流程。
- 本白皮书概述了法案框架，重点介绍了第 14 条带来的关键合规挑战，并介绍了 CMA 检定中心 的自动化合规解决方案。该解决方案旨在帮助企业有效率、准确、大规模地履行报告义务。

1. 欧盟网络韧性法案 (CRA) 概述

《网络韧性法案》(CRA)是欧盟首部涵盖**所有含数字元素产品**的横向网络安全法规。其基础是一项统一原则：

「安全设计」与生命周期网络安全保障结合

关键监管目标

- **安全设计产品：**上市时不存在已知可利用漏洞
- **默认安全性配置**
- **强制性漏洞管理和免费安全性更新**
- **全生命周期网络安全责任**
- **统一的欧盟合规要求，消除分散的国家法规**

覆盖范围

- 硬件产品
- 软件应用
- 相关远程数据处理服务（例如，云端连接的智能家庭系统）

2. 产品范围和风险分类

法案将产品分为三种风险等级，几乎涵盖所有数字产品：

2.1 通用数字产品

所有连网或具备数字化功能的产品，包括：

- 消费性电子产品
- 办公室软件
- 智慧家电

2.2 重要产品（强制性第三方评估）

一级（中度风险）

- 营运系统
- 路由器
- 智慧门锁
- 密码管理器
- 智慧摄影机
- 穿戴式健康设备
- 智能玩具

类别 II（高风险）

- 防火墙
- 入侵检测/防御系统
- 虚拟机管理程序
- 容器运作时系统
- 防篡改处理器和微控制器

2.3 关键产品

- 硬件安全模块 (HSM)
- 安全组件和芯片
- 智能卡
- 智慧电表网关
- 进阶加密设备

这些产品需要根据**欧盟统一框架获得 EUCC 认证**。

3. 承担责任的相关经济体

法案对整个供应链施加了义务及责任：

持份者	责任
生产商	设计、测试、漏洞管理、安全性更新、生命周期合规性
进口商	验证 CE 标志和合规性文件
分包商	确保销售合规产品；报告风险
自有品牌/修改器	承担全部制造商责任
开源维护者	有限义务（仅适用于商业化的开源产品）

4. 不合规的后果

- **罚款：最高可达全球年营业额的 2.5% 或 1,500 万欧元（以较高者为准）**
- **市场执法措施：**
  - 产品禁令
  - 强制召回
  - 退出欧盟市场
- **其他后果：**
  - 没收非法所得
  - 市场准入限制
  - 消费者集体诉讼

5. 关键实施时间表

日期	里程碑	紧急程度	所需操作
2026 年 9 月 11 日	第 14 条强制报告生效	⭑ ⭑ ⭑ ⭑ ⭑	部署事件响应和自动化报告系统
2027 年 12 月 11 日	全面执行《消费者报告法》（强制要求 CE 标志）	⭑ ⭑ ⭑	完成所有产品的合规性认证

6. 第十四条：核心合规挑战

6.1 强制报告触发因素

制造商在以下情况必须报告:

- **已发现被主动利用的漏洞**
  - 现实世界攻击或概念验证（PoC）流传的证据
- **• 发生严重的安全事件**，例如：
  - 恶意代码注入
  - 大规模资料外泄
  - 设备故障

6.2 严格的报告截止日期

截止日期	要求
24 小时内	早期预警通知（发送给国家网络安全事件响应小组和欧盟网络安全局）
72 小时内	详细事件报告（影响、范围、缓解措施）
14 天/1 个月内	最终报告（补救后报告或事件结论）

这些时间节点**为营运带来了极大的压力**，尤其对于需要管理以下事项的全球分布式团队：

- 时区差异
- 周末突发事件
- 语言和监管报告要求

即使是轻微的延误或错误也可能导致**监管处罚或市场退出**。

7. CMA 检定中心：端到端第 14 条合规解决方案

CMA 检定中心 提供**完全符合规范的自动化漏洞报告云端服务**，旨在解决第 14 条规定的操作和技术挑战。

7.1 SBOM 自动化和管理

- 自动产生或汇入**软件物料列表 (SBOM)**
- • 与全球漏洞数据库实时连接
- **10 分钟**内完成所有组件的完整影响分析

7.2 透过 VEX 进行智慧过滤

- 整合**漏洞利用交换平台 (VEX)**
- 自动过滤 **60% 以上的误报**
- 在维持合规准确性的同时，减少报告工作量

7.3 人工智能驱动的报告自动化

- 阶段自动产生符合 ENISA 标准的英文报告：
  - 预警报告
  - 详细报告
  - 最终报告
- 一键人工验证，然后直接提交至 ENISA 平台
- 旨在可靠地满足 24 小时/72 小时的截止日期要求

7.4 端到端可视性和协调揭露

- 实时仪表板，用于：
  - 合规期限
  - 报告状态
- • 整合**协调漏洞揭露（CVD）**入口网站：
  - 统一的内部和外部报告入口

7.5 随时可进行审计的合规性和全天候监控

- 完整的**活动日志记录**，确保符合法规要求
- 自动化合规记录归档
- **全天候监控和警报**，确保零报告漏洞

8. 额外的合规要求

除了第 14 条之外，各组织还必须履行持续义务：

- ✓ **至少 5 年免费安全更新**（工业产品更新时间更长）
- ✓ 强制性 **SBOM 生成和维护**
- ✓ 安全性更新要求：
  - 默认自动更新（消费性产品）
  - 所有产品均提供退出机制
- ✓ 清晰的**支持生命周期披露**和用户通知
- ✓ 违规行为可能面临消费者集体诉讼

9. 结论：必须立即采取行动

CRA 第 14 条规定了**零过渡、零豁免**的要求。所有已在欧盟市场销售的数字产品必须在 **2026 年 9 月 11 日**前符合规定。

未能建立合规机制的组织：

- 事件响应机制
- 自动漏洞报告
- 生命周期安全流程

将面临重大的财务、营运和声誉风险，包括市场排斥。