目　录

一、概述

当前，软件供应链安全依然是网络安全中备受关注的方向，基于自研产品的技术能力和第一手实测数据，奇安信代码安全实验室继续推出《2024 中国软件供应链安全分析报告》，即本系列年度分析报告的第四期。

软件由自主开发的代码与开源代码等第三方代码集成后，形成混源代码，然后通过编译、连接等构建过程形成软件产品，交付给用户使用。在这一软件供应链模型中，每个阶段中的代码或工件都可能引入安全问题，从而导致最终软件供应链安全事件的爆发。

本期报告仍以此模型为基础，分析各阶段的代码安全问题对软件供应链安全性的潜在威胁，分析内容分别在后续的国内企业自主开发的源代码安全状况、开源软件生态发展与安全状况、国内企业软件开发中开源软件应用状况、典型软件供应链安全风险实例分析等章节中呈现。在此基础上，本报告还总结了趋势和变化。与往年报告相比，本期报告在开源软件生态发展与安全部分新增了对 NPM 生态中恶意 开源软件分析的内容；在典型软件供应链安全风险实例部分，通过实 例再次验证了因软件供应链的复杂性，“外来”组件的“老漏洞”发挥“0day 漏洞”攻击作用的状况。感兴趣的读者可重点关注。

1、软件供应链安全攻击手段依然花样百出

过去的一年中，软件供应链安全攻击事件没有丝毫减少的趋势，