美国白宫召开会议讨论
开源软件给软件供应链带来的安全隐患

主要内容：

1. 美国政府担心开源软件漏洞带来安全隐患。
2. 亚马逊、谷歌和微软等 37 家公司支持 Linux 基金会、开放软件安全基金会发布提升开源软件安全性的计划。
3. 谷歌将在 2022 年三季度发布新的云服务帮助用户降低使用开源软件的安全风险。

当前，开源软件在安全性上面临窘境：一是最近几年针对开源软件的网络攻击频发，在 2021 年同比增长 650%；二是开源软件普遍缺乏在安全方面的资源投入，没有维护关键代码安全的正式标准；维护和增强开源软件安全性的工作，大多以“临时”、“自愿”的方式开展。

美国政府担心开源软件漏洞带来安全隐患。在 2021 年末 log4j2 漏洞曝光后，美国白宫于 2022 年 1 月组织了一场“开源软件安全峰会”。这场会议的核心议题是如何支持开源社区、保障开源软件的安全性。会议的核心议题是三个：一是防止代码和开源包中的安全缺陷和漏洞，二是改进发现

缺陷和修复的过程，三是缩短分发和修复程序的响应时间。参加这次会议的人员，除了负责网络和新兴技术的国家安全副顾问、国家网络总监办公室、科技政策办公室、国防部、商务部、能源部、国土安全部、网络安全和基础设施安全局、国家标准与技术研究所和国家科学基金会，还有 Akamai、亚马逊、Apache 软件基金会、苹果、Cloudflare、Meta（Facebook）、GitHub、谷歌、IBM、Linux 基金会、开源安全基金会、微软、甲骨文、RedHat、VMWare。美国总统拜登已将软件安全作为国家优先事项，他的网络安全行政命令要求只有使用安全软件开发生命周期实践并符合特定联邦安全指导的公司才能向联邦政府出售产品。这是美国第一次利用联邦政府的购买力来推动改进软件供应链。

亚马逊、谷歌和微软等 37 家公司支持 Linux 基金会、开放软件安全基金会发布提升开源软件安全性的计划。该计划估计耗资 1.5 亿美元，通过保护开源软件生产、改进漏洞的发现和修复，以及加快生态系统的修补时间等三大举措，支持开源软件维护者，提供工具来提高软件安全性，已达到保护软件供应链的目的。计划要求对开发人员进行安全编程方面的教育和认证，为前 10,000 个开源软件组件创建和维护安全指标，促进软件版本的数字签名，并将 C 和 C++ 等非内存安全的开发语言用诸如 Go 和 Rust 这类更现代的开发语言替代。该计划还呼吁通过资助专家团队在问题发生时协

助开源项目、提供先进的安全工具、资助第三方审查以及协调数据共享，以确定关键组件改进漏洞、展开补救措施。亚马逊、爱立信、谷歌、英特尔、微软和 VMWare 已为该计划投入 3000 万美元的初始资金。

谷歌将在 2022 年三季度发布新的云服务帮助用户降低使用开源软件的安全风险。谷歌会审查自己使用过的开源软件库，将这些“谷歌可控”的开源软件版本提供给用户，以达到降低软件供应链整体安全风险的目的。此外，谷歌云还宣布与开发者安全平台 Snyk 合作，将这个新推出的云服务与 Snyk 的安全方案实现“原生集成”。使用谷歌云安全和软件开发生命周期工具中的客户可以使用 Synk 漏洞、触发操作和补救建议。这样的合作能有效解决 1 月白宫开源软件安全峰会中提及的主要问题。

当前开源世界受西方意识形态控制，我国作为应用开源软件最活跃的国家，应充分意识到开源软件漏洞带来的风险。建立自主可控的软件体系和技术生态，是我国发展自主、可控、安全的数字技术的基石。