CORAX

Corax代码安全分析平台

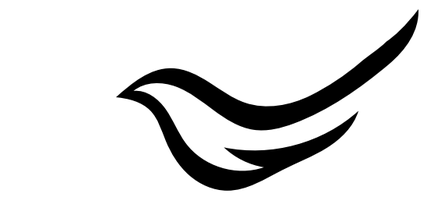
产品白皮书 v2.2.6

2022年10月13日

Corax是由蜚语安全自主研发的静态代码扫描工具，Corax专注于寻找应用源代码中隐藏的复杂高危漏洞。在现代程序分析技术的帮助下，Corax拥有优于传统工具的漏报率与误报率，能够帮助研发人员精准而高效的发现代码中的隐患，提升应用稳定性与安全性。

漏洞挖掘　漏洞管理　低漏报　低误报　高性能

蜚语安全



CORAX

产品白皮书

版本 2.2.6

作者	蜚语安全
文档版本	v2.2.6
页数	5
最后更新时间	2022/10/13
产品版本	v2.2.6

1. Corax静态代码分析平台

Corax是由蜚语安全自主研发的代码安全分析平台，不同于传统基于模式匹配的静态代码分析产品，Corax通过引符号执行、函数摘要、污点分析、路径可达性分析、数据流分析、自然语言处理等前沿的程序分析和人工智能技术增强了自身在处理程序语义信息上的能力，Corax对于代码的建模与分析更加精准高效。Corax采用了模块化的设计理念，更加贴合云原生场景下的现代研发体系，能够方便地嵌入研发流水线的各个环节。通过在研发流程中引入Corax的分析能力，企业能够获得代码安全、代码质量、代码可视化、代码防护等多个方面的研发效能提升。

Corax主要由【扫描管理】平台和【扫描探针】两部分组成。

●【扫描探针】用于执行各式各样的扫描任务，扫描探针一般部署在代码的编译或托管环境中，由用户手动或CI/CD流程自动触发。扫描完成后，扫描探针会基于事先的配置信息，将扫描结果上传至扫描管理平台或用户自建的漏洞管理平台。

●【扫描管理】用于管理各类扫描任务并查看扫描结果。用户可以在扫描管理平台上进行扫描任务管理、结果查看、横向对比、报告导出等多种操作。

2. 产品主要功能

源代码安全分析

Corax在源代码扫描方面能够覆盖多种不同的编程语言与应用构建环境。Corax通过分析源代码的语法、语义信息，发现源代码中存在的中高危安全漏洞。Corax为企业的安全管理人员和研发人员提供强有力的自动化源代码漏洞挖掘能力，帮助企业管理源代码安全，提升企业数字化产品的安全水平。

漏洞生命周期管理

Corax不仅仅能够帮助企业发现代码中的安全问题。在发现安全问题的基础上，Corax还为企业提供了丰富的漏洞管理功能，开发人员或安全管理人员能够基于Corax对源代码的分析结果，对已发现漏洞的全生命周期进行管理，包括但不限于标记漏洞状态、分析漏洞成因、阅读漏洞修复建议、分发漏洞报告、横向对比漏洞数据等。

多用户管理

Corax支持企业对使用人员进行多用户级联管理，可以根据企业内部的架构体系区分不用使用人员的身份，并基于身份对不同的使用人员的权限进行分配管理，满足企业的管理需求。

开放接口

Corax提供全功能的API和CLI接口，用户可以在各类支持API调用的CI/CD平台中调用Corax的相关功能，在不同的场景下触发对源代码的扫描，实时的将扫描结果对接至其他漏洞管理平台，也可以通过企业的工单系统实现对漏洞处置的调度。

3. 产品特性

- **符号执行技术协助降低误报率**

不同于传统的数据流分析技术，Corax会对可能存在数据流依赖的路径进行路径条件的约束求解，消除无法到达的路径，基于Corax特殊优化过的约束求解引擎，能够显著的降低分析误报率。

- **软件代码高精度建模**

Corax会对软件代码中所使用到的外部内存操作函数以及系统库函数进行建模和函数摘要，使Corax在遇到这类外部函数可以更加精确的模拟程序行为，并在更浅的调用层级上定位潜在的高危缺陷与漏洞，显著提升Corax的分析精度和分析速度。

- **跨文件跨模块交叉分析**

Corax会对项目中的所有文件进行预处理，在分析中，Corax会在预处理的结果中找到当前源码文件缺失的函数实现，并进行过程间分析，数据流分析不会因为当前文件缺失函数实现而中断，使得分析更加精确完整

- 专为解决高危安全问题而设计的鸾语定制扫描规则

鸾语安全从现实应用的角度出发，基于对软件安全漏洞和程序分析技术的长时间积累，从主流代码安全规范中筛选出对软件稳定性、安全性影响较大，值得开发人员在软件研发过程中着重注意的代码缺陷与漏洞，形成了鸾语定制规则集。在鸾语定制规则集的帮助下，开发人员能够以较小的代价准确的发现软件代码中潜在的高危安全缺陷和漏洞。

- 多模块并行扫描，提升扫描速度

- 易于使用的UI交互和清晰的漏洞成因描述

Corax专门优化了针对不同类型漏洞的调用流展示，能够让使用人员快速的定位漏洞成因并进行漏洞修复。

- 自定义接口

对于有经验的使用者，Corax提供了丰富的自定义接口（如自定义污点分析source和sink）供用户定制所需要的扫描策略。Corax的常规版本并不开放自定义接口，如果需要使用自定义接口，请直接和我们的售前伙伴联系。

支持语言	C/C++ Object-C Java Python Go PHP	JavaScript C# Kotlin(即将上线) Scala(即将上线) Groovy(即将上线)
支持编译器(C/C++)	Clang GNU GCC/G++ ARM C/C++ TI Code Composer Keil compilers Visual Studio Wind River C/C++ Tasking	GreenHill HighTec Tornado ReDev
支持操作系统	CentOS 7+ Fedora 13+ Ubuntu 16.04+ OpenSUSE 15.4+ Windows 7+ 麒麟桌面/服务器版 统信UOS Deepin 其他Linux	
支持编码标准	CERT C/C++ MISRA 2012 GB/T 38674 GJB 8114	
支持安全标准	MITRE CWE MITRE CWE TOP 10 OWASP TOP 25 ISO 17961 ISO 26262	
分析速度	C/C++: 10万 LoC/分钟 (64核/128G/SSD) Java: 10万 LoC/分钟 (8核/32G/SSD)	
支持单一项目代码上限	~3000万 LoC	

4. 核心价值

源代码安全基线管理

Corax在源代码安全管理方面为企业用户充分赋能。企业的安全管理人员能够通过Corax的定期扫描掌握当前企业中源代码资产的安全情况，及时对源代码资产的安全水平基线进行梳理。在产品上线前用较小的代价发现并修复源代码中的安全问题，减少后续产品运营过程中出现安全事件的风险。

漏洞精准检测与修复

Corax应用了多种前沿的程序分析与人工智能技术，旨在降低对源代码漏洞分析的误报率和漏报率，尽可能的降低研发人员在使用SAST类产品时的额外工作，提升DevSecOps效率。此外，Corax利用数据流分析、符号执行等技术，对每一个漏洞的成因进行了深度分析与追溯，为使用者提供了丰富的调用细节，能够帮助使用者快速理解漏洞成因，增加修复效率。

从0开始搭建DevSecOps体系

Corax作为一款SAST类产品，能够兼容多种编程语言与开发环境。使用时对目标程序的平台与形态没有限制，能够实现高兼容性的自动化并发扫描。Corax的所有分析均离线完成，部署简单，对应用原有的研发流程和运维流程无侵入，不会为服务器带来额外的性能负担。对于尚无DevSecOps体系的企业，Corax非常适合作为第一款左移开发安全产品来帮助提成源代码与应用的安全水平。

提升现有左移开发安全水平

Corax在符号执行、函数摘要、跨文件分析等领域拥有多项核心技术，相比传统的SAST工具，Corax在复杂中高危漏洞挖掘方面拥有更好的表现。同时，Corax也可以和其他的左移开发安全类产品进行协同使用，对于已经开始SDL/DevSecOps体系建设的企业，Corax可以作为原有分析能力的有力补充。

5. 部署方案

Corax具备硬件和软件两种形态，支持本地化部署、私有云/公有云部署。同时，Corax还提供针对小规模代码的单次审计服务，满足中小型企业和大型企业的各类场景需求。

本地部署:

适用场景：企业的CI/CD管道部署在本地，自行管理源代码。

云端部署:

适用场景：企业的CI/CD管道部署在云端，源代码托管在云端。


FEIYU
斐语安全
CORAX