

Know what's in your software.

01 / 04

[HOW IT WORKS]

Resolve. Inspect. Fix in one click.

01

Resolve

Connect a repository and agents parse your lockfiles into the complete dependency graph, capturing every direct and transitive package across every ecosystem you ship.

02

Inspect

Each package is checked against malware intelligence, known advisories and your license policy, then matched to whether your own code actually reaches it.

03

Fix

Every finding ships with the safe version and a pull request that bumps it, so you patch in one click and re-scan the graph instantly.

[SOLUTION ARCHITECTURE]

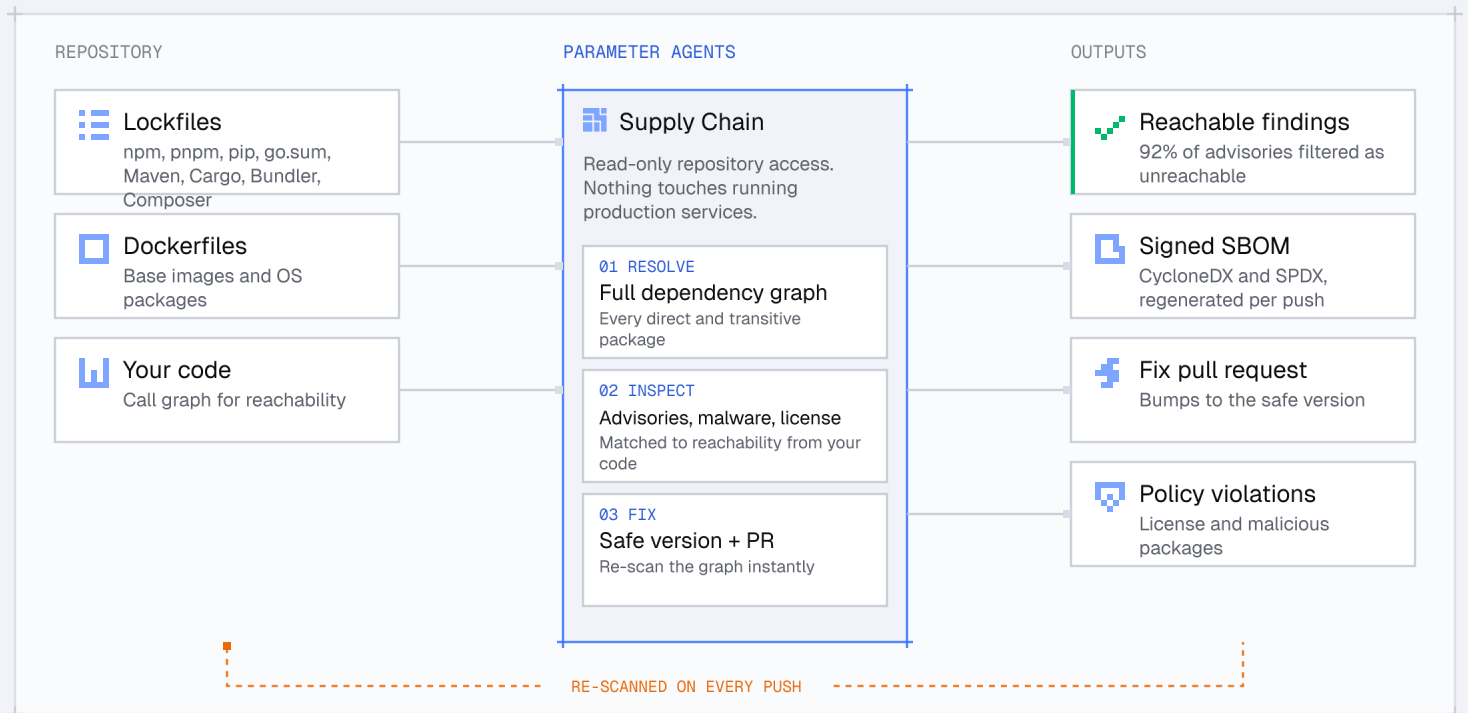


FIG. 01 Supply Chain pipeline. Lockfiles resolve to a full dependency graph; each package is inspected against advisories, malware intelligence and license policy and filtered by reachability from your code; outputs are fix PRs and a signed SBOM.

The graph, not the guesswork

Direct and transitive packages are resolved from lockfiles across every ecosystem, including Go replace directives and container base images.

Only the reachable risk

Parameter traces whether your code can actually reach the vulnerable path. The queue stays short, and every entry is real.

Audit-ready, always current

A signed CycloneDX and SPDX inventory regenerates on every push, so what you attest always matches what you shipped.

[KEY CAPABILITIES]

Every ecosystem you ship.



Reachability analysis

Call-graph and data-flow tracing from your code to the vulnerable function, applied to every advisory.



Malicious package detection

Install scripts, obfuscated payloads and typosquatted names inspected before they run in CI.



Signed SBOM

CycloneDX and SPDX inventory regenerated and signed on every push.



License compliance

Every package matched against your license policy, with violations surfaced alongside security findings.



Container coverage

Base images and OS packages from Dockerfiles resolved into the same graph as application dependencies.



One-click fix and re-scan

A pull request that bumps to the safe version, with the graph re-scanned instantly after merge.

[PRODUCT]

Parameter

Home

Lens Agent

Penetration Tests

Autopilot

Findings

Sentinel

Secret Scanning

Dependencies

Infrastructure

Knowledge

Integrations

Docs

Inbox

Acme

Dependencies > CVE-2026-25896

T1

CVE-2026-25896

reachable uncertain

fast-xml-parser 5.2.5 · npm · acme/core

fast-xml-parser has an entity encoding bypass via regex injection in DOCTYPE entity names

DESCRIPTION

Entity encoding bypass via regex injection in DOCTYPE entity names

Summary

A dot (.) in a DOCTYPE entity name is treated as a regex wildcard during entity replacement, allowing an attacker to shadow built-in XML entities (<lt; , <gt; , <amp; , <quot; , <apos;) with arbitrary values. This bypasses entity encoding and leads to XSS when parsed output is rendered.

Details

The fix for CVE-2023-34104 addressed some regex metacharacters in entity names but missed . (period), which is valid in XML names per the W3C spec.

In DocTypeReader.js , entity names are passed directly to RegExp() :

JavaScript

entities[entityName] = {
 regex: RegExp('<\${entityName}<;', "g"),
 val: val
}

Status Open

VULNERABILITY

Advisory GHSA-m7jm-9gc2-mpf2

CVE CVE-2026-25896

CVSS 9.3

EPSS 0.5%

KEV No

Adjusted Critical

Tier T1

Reachability Reachable

Reach conf. 75%

Exploitability Uncertain

DEPENDENCY

Ecosystem npm

Relationship Transitive

Scope Runtime

Repository Ask Lens

FIG. 02 The dependency graph view: reachable advisories highlighted against the full transitive tree, with the safe version and fix PR for each.

parameter.ai

© 2026 Anytool, Inc. All rights reserved.

03 / 04

[TECHNICAL SPECIFICATIONS]

ACCESS	Read-only repository access only; nothing touches running production services
TRIGGER	Re-scanned on every push
RESOLUTION	Lockfile-based; direct and transitive packages across all ecosystems in the repository
REACHABILITY	Matched to whether your code reaches the vulnerable path
INTELLIGENCE	Malware intelligence, known advisories, license policy
SBOM	Signed CycloneDX and SPDX, regenerated on every push
REMEDIATION	Pull request bumping to the safe version; instant re-scan
ROUTING	Jira, Linear, Slack; shared platform queue

ECOSYSTEMS

- JavaScript and TypeScript
npm, Yarn, pnpm and Bun lockfiles.
- Python, Go, Java and Kotlin
pip, Poetry and uv; Go modules and go.sum including replace directives; Maven and Gradle.
- Rust, Ruby and PHP
Cargo, Bundler and Composer.
- Containers
Base images and OS packages declared in Dockerfiles.

[ECOSYSTEMS AND LOCKFILES]

JS/TS
npm, Yarn, pnpm, Bun

Python
pip, Poetry, uv

Go
go modules, go.sum, replace directives

Java/Kotlin
Maven, Gradle

Rust/Ruby/PHP
Cargo, Bundler, Composer

Containers
Dockerfile base images, OS packages

[WHY PARAMETER]

- ✓ **92% less to triage**
Reachability analysis filters out the advisories your code cannot reach.

✓ **Attestation that matches the build**
Signed SBOM on every push, in both CycloneDX and SPDX.
- ✓ **Malware, not just CVEs**
Packages are inspected for malicious behavior before they run in CI.

✓ **One queue with code, cloud and app findings**
Correlated with Sentinel, Cloud Security and the Pentesting Agent on the same platform.

[PART OF THE PARAMETER PLATFORM]

Supply Chain and Sentinel share the same repository connection. A reachable vulnerable dependency is flagged in the PR that introduces it, and the Pentesting Agent confirms exploitability in the running application.

See first findings in 24 hours.

ABOUT PARAMETER

Parameter is an AI-powered security platform that continuously finds and validates vulnerabilities before attackers can exploit them. Autonomous agents pentest like a real adversary across your code, cloud and dependencies, with every finding proven. Formerly Hex Security, Parameter is backed by Y Combinator and built by a team that has secured Apple, Google, Microsoft, the U.S. Department of Defense, T-Mobile, Henkel, Epic Games, AT&T and Yahoo.

TRUST AND COMPLIANCE

SOC 2 Type I (Type II observation underway)
HIPAA BAA available
GDPR DPA with SCCs
Data processed in the US
parameter.ai · support@parameter.ai · app.parameter.ai