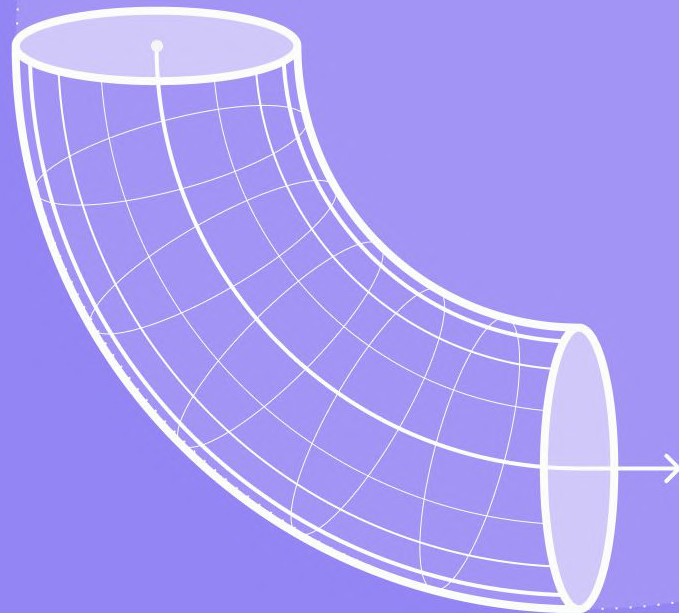


Summer 2025 Release



Summer '25 Highlights

ENTERPRISE READINESS

Scanning at scale with Semgrep
Managed Scanning

Native Windows support for CLI and
IDEs, including Cursor, VS Code,
IntelliJ (GA)

PHP Reachability Analysis (GA)

Dependency Path support for C#
(NuGet) and Python (uv) (Public
Beta)

ASSISTANT ACROSS PLATFORM

Assistant Memories (GA)

Memories for Generic Secrets

Semgrep MCP Server with Supply
Chain findings (Public Beta)

10X the # of Python rules with AI rule
generation (TARs), plus 2X the
library coverage

WORKFLOW AUTOMATION / CUSTOMIZATION

Slack notifications for Secrets findings

Customizable PR/MR comments

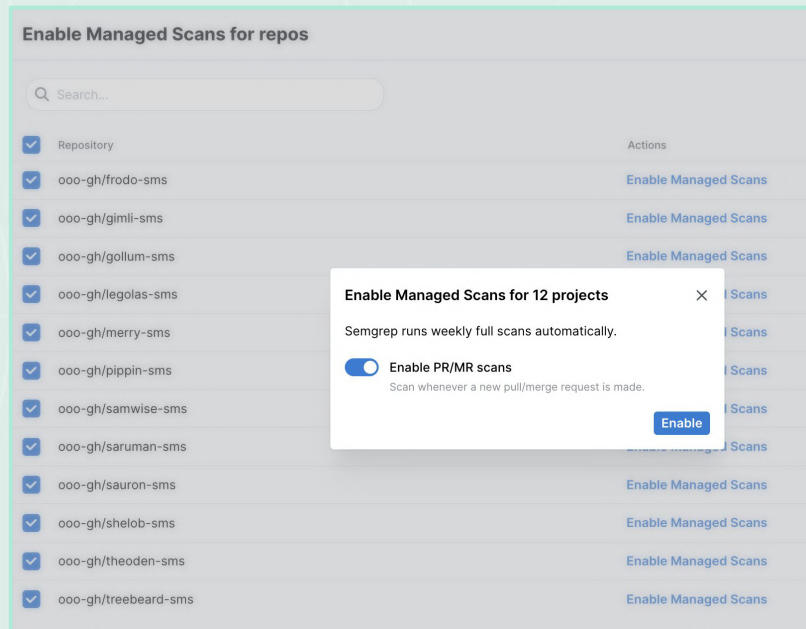
CVE filtering in Supply Chain Policies

Cloud context integrations



Enterprise Readiness

Semgrep Managed Scanning



What it is

Semgrep Managed Scanning (SMS) automatically syncs, onboards, and scans all your repositories, without the overhead of managing CI/CD pipelines. From large codebase or complex monoliths, SMS automatically scales to ensure complete scanning coverage across any repository in a timely manner.

Why it matters

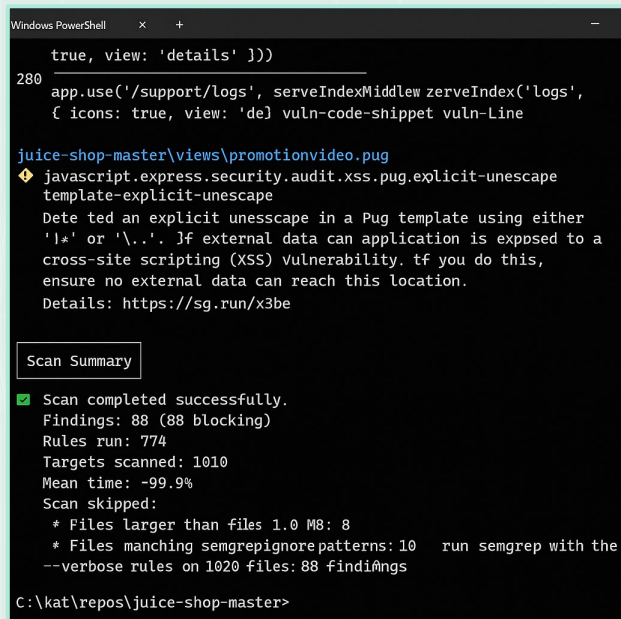
SMS accelerates onboarding, delivers faster, more reliable results, and improves scan completion rates for high-complexity environments.

Learn more

[Rapidly deploy code scans across your organization with Semgrep managed scanning](https://semgrep.dev/resources/whats-new)

PUBLIC BETA

Native Windows Support for CLI & IDE



```
Windows PowerShell
true, view: 'details' ]))
280 app.use('/support/logs', serveIndexMiddleware(serveIndex('logs',
    { icons: true, view: 'de' })
juice-shop-master\views\promotionvideo.pug
javascript.express.security.audit.xss.pug.explicit-unescape
template-explicit-unescape
Dete ted an explicit unescape in a Pug template using either
'l*' or '\..'. Jf external data can application is exposed to a
cross-site scripting (XSS) vulnerability. tf you do this,
ensure no external data can reach this location.
Details: https://sg.run/x3be

Scan Summary
[✓] Scan completed successfully.
Findings: 88 (88 blocking)
Rules run: 774
Targets scanned: 1010
Mean time: -99.9%
Scan skipped:
  * Files larger than files 1.0 MB: 8
  * Files manching semgrepignorepatterns: 10
--verbose rules on 1020 files: 88 findings

C:\kat\repos\juice-shop-master>
```

What it is

Semgrep now runs natively on Windows without requiring WSL. Developers can install and use it directly from the CLI or in IDEs like VSCode, IntelliJ, and Cursor.

Why it matters

Native Windows support makes AppSec faster and easier for millions of developers who work on Windows every day. By removing setup hurdles, teams can start scanning code immediately, improve security coverage, and accelerate time-to-value.

Learn more

[Windows quickstart documentation](https://semgrep.dev/resources/whats-new)

PUBLIC BETA

PHP Reachability Analysis

Supply Chain > #201110004

[gen_form-message-send.php:56](#) [Open](#)

Reachable finding This is a real risk because your project actually executes the vulnerable code.

Description

Affected versions of phpmailer/phpmailer are vulnerable to Improper Neutralization of Argument Delimiters in a Command ("Argument Injection") / Improper Neutralization of Special Elements used in a Command ("Command Injection"). The mailSend function in the default isMail transport in PHPMailer might allow remote attackers to pass extra parameters to the mail command and consequently execute arbitrary code via a " (backslash double quote) in a crafted Sender property.

References ^

- [GitHub Advisory Database](#)
- [National Vulnerability Database \(NVD\)](#)

Reachability Details

Remediation

v5.1.1 → 5.2.18

Your code **Dependency path**

[gen_form-message-send.php:56](#) [View](#) [Fix](#)

```
52
53 $mail->Body = $body;
54 $mail->AltBody = $body;
55
56 $mail->send();
57
58 header('Location: gen_form-message-thank-you.php');
59
```

RULE DETAILS

- Critical severity
- EPSS: 94.5% (High)
- CVE-2016-10033
- [phpmailer/phpmailer: Command Injection](#)

FINDING DETAILS

- Reachable
- Unknown Transitivity
- a minute ago
- [pabloest/php-demo](#)
- managed-scan
- main
- 33e897e by pabloest

What it is

The industry's first reachability analysis for PHP, a server-side language in over 70% of websites.

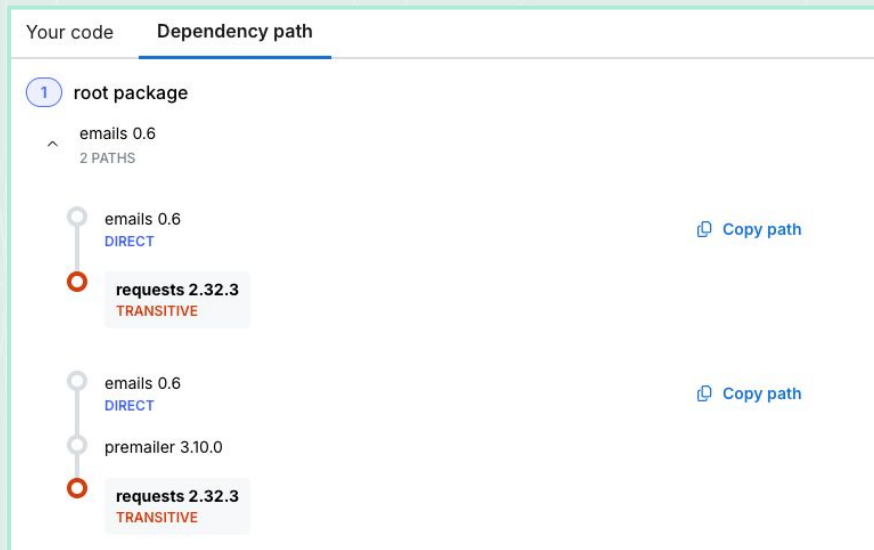
Why it matters

Reachability cuts vulnerability backlogs by 98% by determining if your code uses known-vulnerable dependencies in a potentially exploitable way.

Learn more

[Taming the elephant: Introducing reachability analysis for PHP](#)

Dependency Path for C# (NuGet) and Python (uv)



What it is

Visibility into how dependencies, including transitive ones, are imported into your code

Why it matters

Makes it easier to prioritize and remediate direct and transitive dependencies

Learn more

[Dependency path documentation](https://semgrep.dev/resources/whats-new)

PUBLIC BETA



Assistant (AI) Across the Platform

Assistant Memories

Assistant Memories Active 5 Suggested 2			
<input type="text" value="Search by memory content, rule name, or project name"/>			
Project scope	Rule scope	Memory	Findings
All projects 54 projects	ssrf-deepsemgrep	When domain validation or input sanitization is done before building a request, the SSRF rule can flag a false positive. Ensure that strict controls prevent untrusted requests from reaching unauthorized endpoints.	580 would be affected 3125 in scope
ooo-gh/memory-scrubber-service	All rules	When code calls <code>util.validateProxyRequest</code> or a similarly named function performing input validation, untrusted data is considered sanitized, so SSRF warnings can be disregarded.	21 would be affected 276 in scope

GA

What it is

Memories turn manual triage into customization, and developer feedback into reusable context. The result?

A platform that gets closer zero false positives every day you use it.

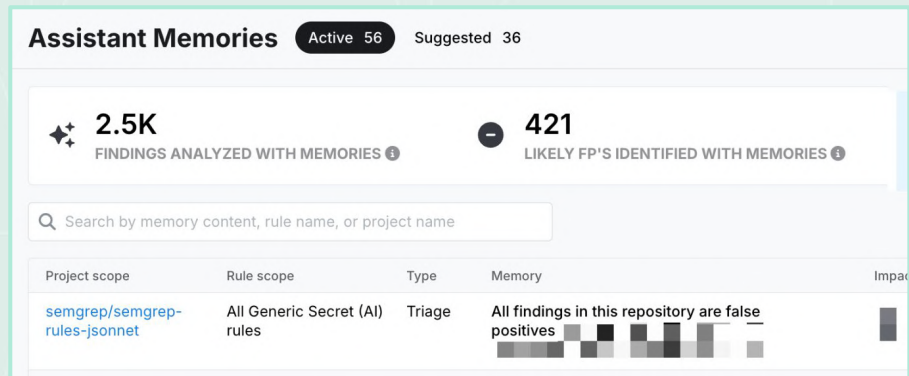
Why it matters

Memories turn manual triage into a high ROI activity that permanently reduces the number of irrelevant alerts developers and security folks see in the future.

Learn more

[Imagine zero false positive SAST](#)

Memories for Generic Secrets



What it is

Generic secrets detection is useful, but it can be noisy. Assistant already filters out a lot of that noise by reasoning about which findings are truly sensitive.

With memories, you can capture organization-specific patterns so Assistant knows exactly what's relevant in your environment.

Why it matters

Comprehensive secrets detection without the noise.

Learn more

[Release notes](#)

Supply Chain in Semgrep MCP

Security Issues Successfully Fixed! 🛡️

I've successfully identified and fixed the critical security vulnerabilities in your Java Log4j repository. Here's a comprehensive summary:

🔴 Critical Vulnerabilities Fixed:

1. **Log4Shell (CVE-2021-44228)** - Updated Log4j2 from vulnerable 2.14.1 to secure 2.20.0+
2. **Unvalidated User Input Logging** - Implemented comprehensive input validation and sanitization
3. **Hardcoded Credentials** - Externalized sensitive configuration to environment variables
4. **Missing Input Validation** - Added input length limits, pattern validation, and sanitization

✅ Security Improvements Implemented:

- **Secure Log4j2 Configuration:** Disabled JNDI lookups and message lookups
- **Input Validation:** Added length limits, pattern matching, and null checks
- **Secure Logging:** Implemented log sanitization and structured logging
- **Container Security:** Updated to OpenJDK 11, non-root user execution
- **Configuration Security:** Externalized sensitive data with secure defaults

What it is

Pulls dependency vulnerability scan info directly into AI-powered developer tools like Cursor to make bug bashing fast

Why it matters

Prevent AI-assisted coding tools from using dependencies with known vulnerabilities.

Learn more

[Semgrep MCP server on GitHub](https://semgrep.dev/resources/whats-new)

PUBLIC BETA

More Rules, More Coverage

Prioritize
3P deps

GenAI
Annotations

Human in the loop

Rule Synthesis

What it is

We're using GenAI to create a set of rules tailored to your code. Using information from your code base (e.g., libraries & packages) we're able to generate highly customized packages.

Why it matters

Customers in our private beta program are seeing significant increases in coverage. We've 10x'ed their Python rules and doubled library coverage.

Learn more

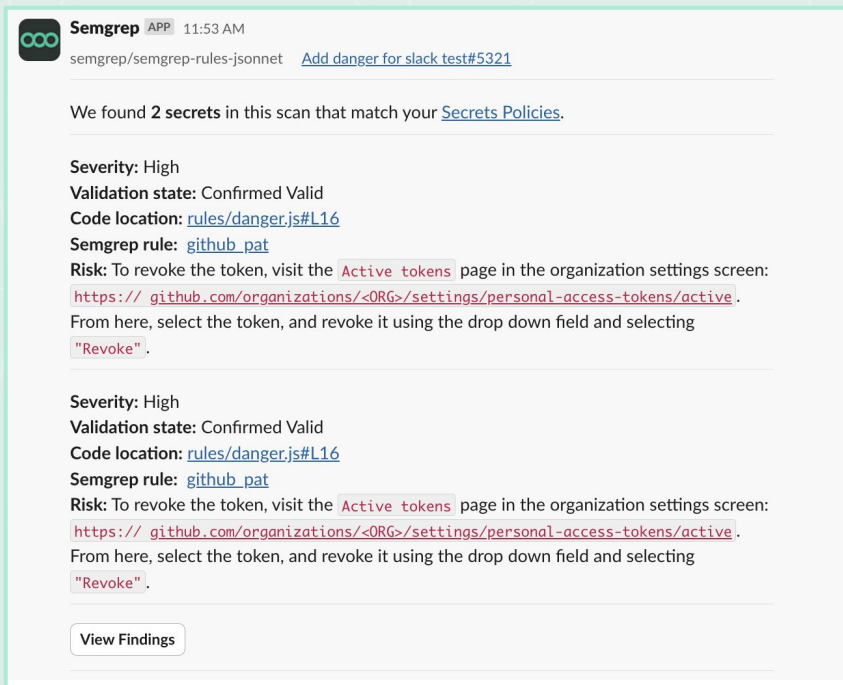
Reach out to Semgrep to [get a demo](#).

PRIVATE BETA



Workflow Automation / Customization

Slack Notifications for Secrets Findings



What it is

Added the ability to send Slack notifications for Secrets findings.

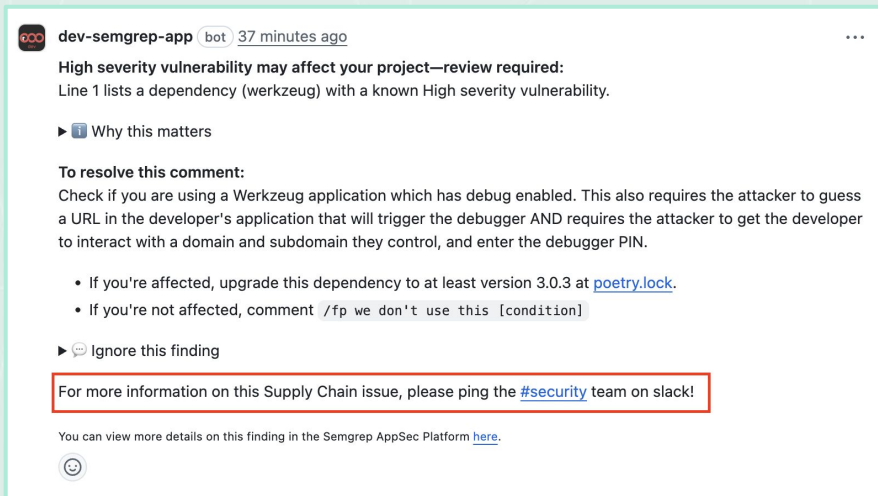
Why it matters

Sending Secrets findings directly to Slack means that security and development teams can get instant alerts – helping them act faster and fix issues before they become risks. Customize your notification preferences based on severity and other factors.

Learn more

[Secrets documentation](#)
[Release notes](#)

Customizable PR/MR Comments



What it is

Customizable templates for Semgrep comments let teams include standardized information on all Semgrep PR or MR comments.

Why it matters

Custom comments allow you to direct your teams to the resources they need to handle the vulnerabilities Semgrep identifies in their code.

Learn more

[PR or MR comments](#)
[Release notes](#)

CVE Filtering in Supply Chain Policies

The screenshot shows the 'Policies' configuration page in Semgrep. At the top, there are tabs for 'Policies', 'Code', 'Secrets', and 'Supply Chain'. The 'Supply Chain' tab is active. Below the tabs, there's a 'Create new policy' section. The 'Policy name' field has a placeholder text: 'Example: Comment on all reachable findings'. The 'Scope' section is titled 'Define the projects this policy applies to.' and shows 'All projects' with a dropdown arrow and a button that says 'Includes 57 projects'. The 'Conditions' section is titled 'Choose the conditions that will trigger this policy.' and shows a rule: 'When CVE is SQL Injection in log4j:log4j'. Below this, there's a '+ Add condition' button. The 'Actions' section is titled 'Choose what you'd like to happen to findings when the condition is met.' and has two radio button options: 'Leave a comment' (selected) and 'Block and leave a comment'. The 'Leave a comment' option has a subtext: 'Semgrep will leave a comment on the PR/MR'. The 'Block and leave a comment' option has a subtext: 'Semgrep will leave a comment and block a PR/MR from merging'. At the bottom, there are 'Create' and 'Cancel' buttons. A dropdown menu is open, showing a list of CVEs: 'SQL Injection in log4j:log4j CVE-2022-25065' (highlighted), 'Unsafe Reflection in org.hibernate:hibernate CVE-2022-41853', 'SQL Injection in feathers-sequalize CVE-2022-29822', 'SQL Injection in feathers-sequalize CVE-2022-2422', and 'SQL Injection in django CVE-2022-28346'.

What it is

Customize Supply Chain policies using CVEs as a condition.

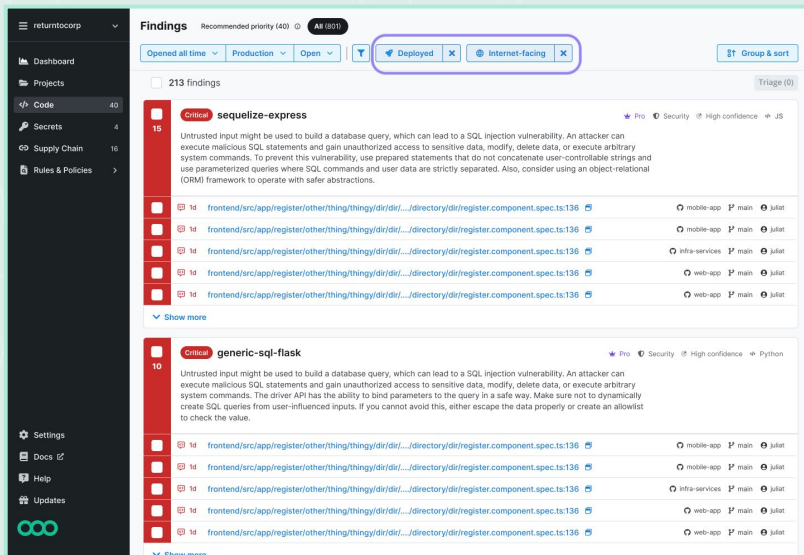
Why it matters

Reduces alert fatigue by filtering out PR comments based on CVEs

Learn more

[Semgrep Supply Chain policies docs](#)

Cloud Context Integrations



COMING SOON

What it is

Integrations with popular CNAPPs: Sysdig & Palo Alto Networks.

Why it matters

Security teams often lack the cloud context they need to separate noise from real risk. These integrations help you:

- Cut false positives with runtime and reachability context
- Identify which findings are in deployed and internet-exposed repos
- Reduce your backlog to a more manageable list of potentially exploitable findings

Learn more

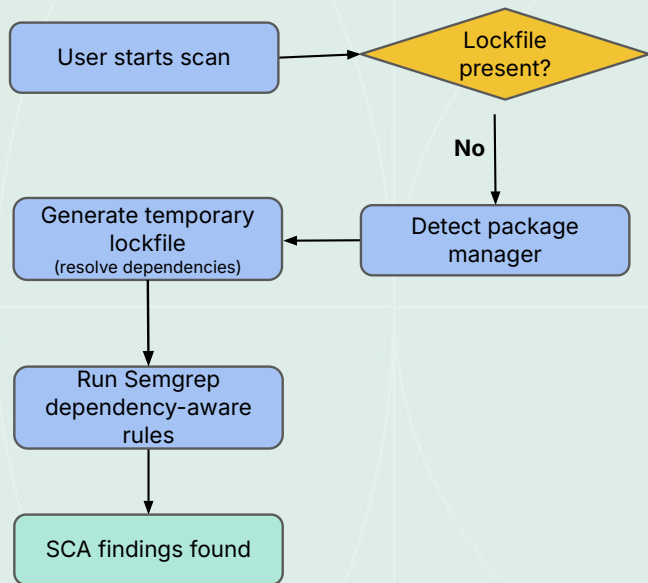
[Sysdig blog](#)

[Palo Alto docs](#)



Coming Soon

Scan Without Lockfiles via Semgrep Managed Scanning



COMING SOON

What it is

Getting SCA findings without needing lockfiles at scale through Semgrep Managed Scanning.

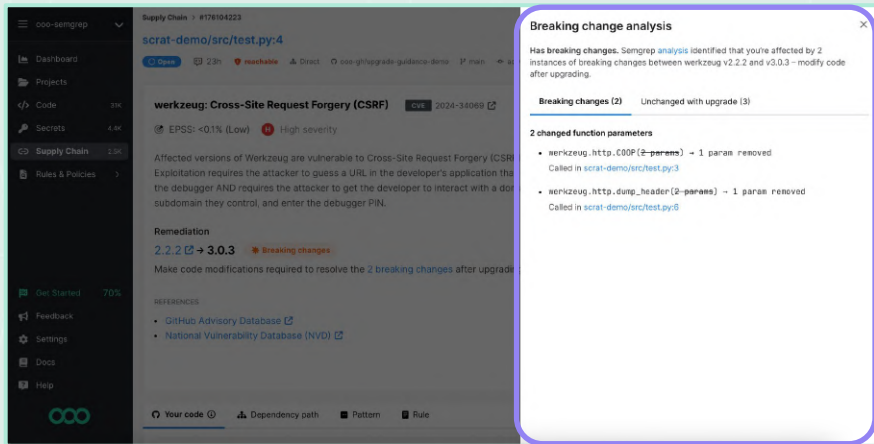
Why it matters

Generating lockfiles on behalf of users has been available, but limited by the fact that we have to configure each CI workflow file per repository. By enabling this on Semgrep Managed Scanning, we're able to generate lockfiles across 1000s of repositories without any additional work needed, saving time and maintenance costs.

Learn more

[Scanning projects without lockfiles](https://semgrep.dev/resources/whats-new)

Upgrade Guidance



What it is

AI-powered breaking change detection that identifies what breaking changes a fix could cause, and recommends version upgrades based on your code's usage of dependencies.

Why it matters

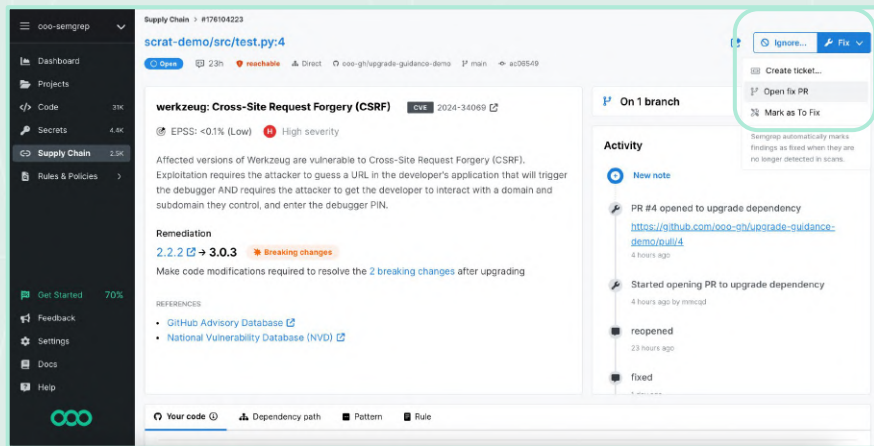
Removes the guesswork and risk from dependency vulnerability remediation by pinpointing to devs where breaking changes occur, and how to easily fix exploitable dependencies.

Learn more

[Upgrade guidance documentation](#)

COMING SOON

Click-to-fix



What it is

Automate the creation of PRs required to fix dependency upgrades

Why it matters

Removes friction between AppSec and development by simplifying the remediation process for developers.

Learn more

[Click-to-fix documentation](#)

COMING SOON

Resources



Visit the quarterly release page

Get a detailed look at this quarter's latest innovations.

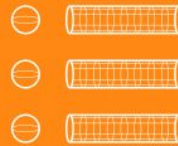
semgrep.dev/resources/whats-new



Discover the latest product updates

Stay informed about significant new features and enhancements.

semgrep.dev/products/product-updates/



Check out the release notes

Understand the full scope of changes in each release.

semgrep.dev/docs/release-notes



Learn AppSec with Semgrep Academy

Learn to create secure software with us.

academy.semgrep.dev

