

Introducing OWASP OASIS: Initiative Fighting Back Against AI and Human Exploits of Open Source Software Vulnerabilities

Global initiative fights AI with AI and AppSec community expertise, implementing AI-generated fixes to remediate open source vulnerabilities at scale

SAN FRANCISCO, CA, UNITED STATES, August 26, 2026 /EINPresswire.com/ -- Today, a community

“

Open source powers the information economy, yet unremediated vulnerabilities put critical infrastructure at risk. OASIS enables AppSec and open source communities to deliver secure software together.”

Chris Holt, Strategic Engagement and Community Architect at Intigriti.

of application security professionals launched [OWASP](#) Open Automated Security Initiative for Software ([OASIS](#)). This global initiative marshals human expertise to deliver crowd-validated vulnerability fixes for the open source software that underlies 98% of commercial codebases, including critical infrastructure and commercial software. OWASP OASIS combines donated AI-powered fix automation and validation tooling with human expertise to move open source security from discovery to immediate remediation at scale.

OASIS has attracted hundreds of AppSec professionals from a variety of industries, alongside founding industry members [AppSecAI](#), Intigriti, and DryRun Security.

“Open source underlies the vast majority of our information economy,” said Chris Holt, Strategic Engagement and Community Architect at Intigriti. “Because of the nature of the development process, unremediated vulnerabilities put a huge segment of our critical software infrastructure at risk. OASIS enables AppSec and open source communities to cooperatively deliver secure open source software together.”

What OWASP OASIS Is

For decades, the security industry has focused on finding vulnerabilities. The bottleneck has always been remediation: the cost, process complexity, and specialized expertise required to deliver credible security fixes for vulnerabilities.

OASIS changes that by leveraging Fix Automation and Validation, an emerging category of AI tools that generate and validate candidate fixes as vulnerabilities are found. OASIS’s community-

driven validation layer makes those fixes trustworthy for upstream developer validation and contribution.

The three-part process:

1. AI Pipeline: Automated tools scan open source repositories and generate candidate security fixes at scale. Found vulnerabilities always come with a candidate fix
2. Expert Community Validation: The community reviews fixes, assesses correctness and safety, and determines which ones are credible, reducing validation time to minutes
3. Upstream Contribution: Validated fixes are provided to open source teams as credible, community-validated security patches for consideration, allowing maintainers to quickly validate them for functionality and performance and integrate them at their discretion

By generating code fixes while contributing to the open source ecosystem, OASIS democratizes the vulnerability remediation process with a collaborative platform to augment human capabilities and improve security fixes at scale.

"It's always been easier to find than to fix," said Michael Cartsonis, Co-Founder and VP of Product at AppSecAI. "What OASIS does is give those with code security experience the agency to participate. Now, in just a few minutes, you can contribute. We are excited to help the OASIS community protect the software that quite literally runs the world."

Why Now?

The launch of OASIS comes at a defining moment. "Vibe hacking," the AI-assisted discovery and exploitation of vulnerabilities, enables attackers to move faster than security teams can respond. However, the same generative AI powering attacks offers a defense: the AppSec community now has the power to find and generate validated fixes at comparable speed.

"AI is dramatically increasing the speed at which software is created, and it's also increasing the speed at which vulnerabilities can be discovered and exploited," said James Wickett, CEO and Co-Founder of DryRun Security. "OASIS is an important step toward giving defenders the same advantage. By combining AI-powered remediation with independent validation and the expertise of the AppSec community, we can turn vulnerability discovery into credible fixes that maintainers can actually use. We're proud to support OASIS and help move open source security from finding more problems to fixing them at scale."

This reality has catalyzed complementary initiatives across the industry. Frontier AI developments like Anthropic's Project Glasswing introduced highly advanced models like Claude Mythos to defenders, while OpenAI's Patch the Planet and the Linux Foundation's Akrites have mobilized elite research teams and tech coalitions to protect core software infrastructure.

While these programs focus on researcher-led intervention for select high-priority infrastructure, OASIS is open, democratic, and vendor-agnostic. It leverages volunteers from the AppSec community to scale broadly across the open source landscape and address the long tail of software libraries and applications used by enterprises.

Why Open Source Needs OWASP OASIS

Open source maintainers face an onslaught of low-fidelity information.

OASIS acts as a community quality filter. AppSec experts assess whether a candidate fix is accurate and safe. Human validation converts rapid AI output into a patch a maintainer can trust. It provides a straightforward, vendor-neutral way for AppSec professionals to give back to the open source community.

Why Enterprise Users need OWASP OASIS

Open source code underlies countless custom enterprise applications. When that code is vulnerable, they are exposed, dependent on maintainers to keep organizations running.

"I have spent thirty years defending enterprises, and every one of them builds on open source components, which means every one of them inherits any unfixed vulnerabilities in that code. Our industry got very good at finding problems and never solved fixing them at scale," said David Kosorok, Director of Product Security at ACV Auctions. "That is what OASIS changes. When the community validates a fix and it lands upstream, thousands of applications get safer at once. That is the highest-leverage work an application security professional can do, and now it is open to all of us."

How to Get Involved

Join the initiative at owasp-oasis.org

About OWASP OASIS

The Open Automated Security Initiative for Software (OASIS) is a vendor-neutral, community-driven initiative that mobilizes the Application Security community to deliver validated vulnerability fixes for the open source software that runs the world. By combining AI-powered fix automation with human expert validation, OASIS moves open source security from discovery to remediation at scale. OASIS is an OWASP project.

OWASP does not endorse any product, services, or tools.

About OWASP

The OWASP Foundation is a nonprofit organization that works to improve software security. Through community-led open source software projects, over 260 local chapters worldwide, tens of thousands of members, and leading educational and training conferences, the OWASP Foundation is the source for developers and technologists to secure the web. For nearly two decades, corporations, foundations, developers, and volunteers have supported the OWASP Foundation and its work. To learn more or to become a member, visit owasp.org.

Media Contact

Kira Wojack

kira@merrittandrose.com

+1 415-419-4062

Kira Wojack

Merritt and Rose

+1 415-419-4062

[email us here](#)

Visit us on social media:

[LinkedIn](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/937025119>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2026 Newsmatics Inc. All Right Reserved.